

# Complex Linear Physical-Layer Network Coding

Long Shi, *Member, IEEE* and Soung Chang Liew, *Fellow, IEEE*

**Abstract**—This paper presents the results of a comprehensive investigation of complex linear physical-layer network (PNC) in two-way relay channels (TWRC). In this system, two nodes A and B communicate with each other via a relay R. Nodes A and B send complex symbols,  $w_A$  and  $w_B$ , simultaneously to relay R. Based on the simultaneously received signals, relay R computes a linear combination of the symbols,  $w_N = \alpha w_A + \beta w_B$ , as a network-coded symbol and then broadcasts  $w_N$  to nodes A and B. Node A then obtains  $w_B$  from  $w_N$  and its self-information  $w_A$  by  $w_B = \beta^{-1}(w_N - \alpha w_A)$ . Node B obtains  $w_B$  in a similar way. A critical question at relay R is as follows: “Given channel gain ratio  $\eta = h_A/h_B$ , where  $h_A$  and  $h_B$  are the complex channel gains from nodes A and B to relay R, respectively, what is the optimal coefficients  $(\alpha, \beta)$  that minimizes the symbol error rate (SER) of  $w_N = \alpha w_A + \beta w_B$  when we attempt to detect  $w_N$  in the presence of noise?” Our contributions with respect to this question are as follows: (1) We put forth a general Gaussian-integer formulation for complex linear PNC in which  $\alpha, \beta, w_A, w_B$ , and  $w_N$  are elements of a finite field of Gaussian integers, that is, the field of  $\mathbb{Z}[i]/q$  where  $q$  is a Gaussian prime. Previous vector formulation, in which  $w_A, w_B$ , and  $w_N$  were represented by 2-dimensional vectors and  $\alpha$  and  $\beta$  were represented by  $2 \times 2$  matrices, corresponds to a subcase of our Gaussian-integer formulation where  $q$  is real prime only. Extension to Gaussian prime  $q$ , where  $q$  can be complex, gives us a larger set of signal constellations to achieve different rates at different SNR. (2) We show how to divide the complex plane of  $\eta$  into different Voronoi regions such that the  $\eta$  within each Voronoi region share the same optimal PNC mapping  $(\alpha_{opt}, \beta_{opt})$ . We uncover the structure of the Voronoi regions that allows us to compute a minimum-distance metric that characterizes the SER of  $w_N$  under optimal PNC mapping  $(\alpha_{opt}, \beta_{opt})$ . Overall, the contributions in (1) and (2) yield a toolset for a comprehensive understanding of complex linear PNC in  $\mathbb{Z}[i]/q$ . We believe investigation of linear PNC beyond  $\mathbb{Z}[i]/q$  can follow the same approach.

**Index Terms**—Complex linear physical-layer network coding, Gaussian integer, minimum distance, Voronoi region

## I. INTRODUCTION

Physical-layer network coding (PNC) can potentially boost the throughput of relay networks, such as a two-way relay channel (TWRC) [1], [2]. Linear PNC allows PNC decoding to be performed in a simpler manner than nonlinear PNC. In TWRC, data exchange between two isolated nodes A and B is facilitated by a relay R. When PNC is employed in TWRC, the data exchange consists of two phases. In the uplink phase, nodes A and B transmit  $w_A$  and  $w_B$  to relay R simultaneously. For linear PNC, the relay aims to decode a linear combination of  $w_A$  and  $w_B$  as a network-coded (NC) symbol,  $w_N = \alpha w_A + \beta w_B$ , from the simultaneously received signals. We refer to the linear combination  $w_N = \alpha w_A + \beta w_B$  as a linear PNC mapping. Equivalently, we also refer to the coefficient pair  $(\alpha, \beta)$  as a PNC mapping, with the understanding that the coefficients are used in the linear combination  $w_N = \alpha w_A + \beta w_B$ . In the downlink phase, relay R broadcasts

$w_N$  to the nodes A and B. Node A then obtains  $w_B$  from  $w_N$  and its self-information  $w_A$  by  $w_B = \beta^{-1}(w_N - \alpha w_A)$ . Node B obtains  $w_A$  by  $w_A = \alpha^{-1}(w_N - \beta w_B)$ .

Linear PNC has been extensively studied because of its scalability in terms of the network coding operation for high-order modulations [1]–[11]. The original version of linear PNC mapping was formulated as binary XOR mapping with BPSK [1]–[5]. This was later extended to higher-order signal modulations [8]–[11]. Prior work in [1]–[7] assumed ideal communication scenarios in which signals of the two end nodes received at the relay have balanced powers with perfect phase alignments. However, these ideal scenarios rarely occur in practice because of factors such as imperfect power control, relative carrier frequency offset, and phase noise induced by the use of different oscillators at nodes A and B. In general, the powers will not be perfectly balanced and the phases will not be perfectly aligned.

The authors of [10] formulated a PNC scheme to take into account imbalanced received powers and relative phase offset, assuming the use of  $q$ -PAM and  $q^2$ -QAM modulations by the nodes A and B, where  $q$  is a prime integer. Building on [10], we investigated the error performance of  $q$ -PAM linear PNC in [11] via a systematic analysis of the effect of power imbalance on a signal-constellation minimum distance that characterizes the symbol error rate (SER) of decoding  $w_N$  at the relay. In particular, in [11], we found that the performance of  $q$ -PAM linear PNC can be highly sensitive to small changes in the channel gains (i.e., small variations in channel gains of the two end nodes can cause significant performance changes).

This paper further extends the work in [11]. Whereas [11] assumed real channels for the two end nodes (i.e., the channel gains are real and there is no relative phase offset between them; there is only power imbalance), this paper assumes complex channels to take into account possible relative phase offset between the end nodes besides the power imbalance. We present a comprehensive investigation of optimal complex linear PNC. Our main contributions are as follows:

- **Gaussian-integer formulation**—We put forth a Gaussian-integer formulation for the complex linear PNC mapping in the finite field of Gaussian integer, where  $\alpha, \beta, w_A, w_B \in \mathbb{Z}[i]/q$ , where  $q$  is a Gaussian-integer prime. Compared with the vector formulation in [9], our Gaussian-integer formulation yields more choices of signal constellations for use in complex linear PNC. Specifically, the complex linear PNC in [10] is a subset of the complex linear PNC here: specifically, the vector formulation in [10] is equivalent to our Gaussian-integer formulation with  $q$  being limited to a real prime; in general,  $q$  can be a complex prime in our Gaussian-integer formulation, yielding additional signal constellations that can be used in complex linear PNC mappings. In this

paper, we also recast linear PNC using the coset theory to uncover the isomorphism among different linear PNC mappings. Beyond the mapping arithmetic in [9]–[11], the coset theory offers us with a new angle to understand the principle of linear PNC mapping.

- *Characteristic difference*—We put forth the concept of characteristic difference that is fundamental to the study of optimal PNC mapping and the minimum distance between constellation points that determines the SER performance of  $w_N$ . Specifically, a *characteristic difference* is the difference between two distinct joint symbols,  $(\delta_A^{char}, \delta_B^{char}) = (w_A, w_B) - (w'_A, w'_B)$ , such that there is no common Gaussian-integer factor between  $\delta_A^{char}$  and  $\delta_B^{char}$  (i.e.,  $\gcd(\delta_A^{char}, \delta_B^{char}) = \text{unit}$ ). Given a set of joint symbols,  $\mathcal{W}_{(A,B)} = \{(w_A, w_B) | w_A, w_B \in \mathbb{Z}[i]/q\}$ , there is a corresponding set of characteristic differences encompassing all possible characteristic differences under all possible joint symbols. For a given channel-gain ratio  $\eta = \frac{h_A}{h_B}$ , where  $h_A$  and  $h_B$  are the complex channel gains from nodes A and B to relay R respectively, the minimum distance between any two constellation points in the received overlapped signals,  $l_{\min}$ , is given by the particular characteristic difference that yields the minimum  $|\eta\delta_A^{char} + \delta_B^{char}|$ . The optimal PNC mapping  $(\alpha_{opt}, \beta_{opt})$  for that  $\eta$  is the mapping that maps two pairs of symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  separated by that  $(\delta_A^{char}, \delta_B^{char})$  to the same NC symbol (i.e.,  $w_N = \alpha_{opt}w_A + \beta_{opt}w_B = \alpha_{opt}w'_A + \beta_{opt}w'_B$ ). Hence, there is no need to distinguish between the constellations points corresponding to  $(w_A, w_B)$  and  $(w'_A, w'_B)$  as far as the decoding of  $w_N$  is concerned. As a result,  $l_{\min}$  is not a concern. What matters to SER performance is the minimum distance  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  between two pairs of symbols  $(w_A, w_B)$  and  $(w''_A, w''_B)$  mapped to different NC symbols under  $(\alpha_{opt}, \beta_{opt})$ . For complex linear PNC, *characteristic difference* is more convenient for the identification of the optimal PNC mapping and the study of  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  than the *reference symbol* used in [11], which was devised for the study of real linear PNC.
- *Voronoi-region characterization of optimal PNC mapping*—For a global understanding of  $l_{\min}$  and  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  for all  $\eta$ , we investigate how the complex plane of  $\eta$  can be divided into different Voronoi regions. Associated with the  $\eta$  within each Voronoi region is a characteristic difference  $(\delta_A^{char}, \delta_B^{char})$  that determines the  $l_{\min}$  within that region, and an optimal PNC mapping that causes  $l_{\min}$  to be not a performance concern, as explained in the previous paragraph. We developed a systematic approach to identify the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  for all  $\eta$  within a Voronoi region by considering the characteristic differences associated with the Voronoi regions adjacent to it.

The remainder of this paper is organized as follows. Section II overviews prior related work. Section III describes the general idea of complex linear PNC and raises the key outstanding problems. Section IV presents the advantages of the Gaussian-integer formulation over the vector formulation in complex linear PNC systems. Section V characterizes the optimal PNC

mappings for  $\eta$  at which  $l_{\min} = 0$  and identifies the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  for these  $\eta$  after the optimal PNC mappings. Section VI considers the overall complex plane of  $\eta$  and partitions it into different Voronoi regions. In particular, we show in Section VI that the continuum of  $\eta$  within each Voronoi region has the same optimal PNC mapping. Importantly, we give a systematic approach to finding the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  for the  $\eta$  within each Voronoi region.

## II. RELATED WORK

In the previous few paragraphs, we have reviewed prior work on linear PNC that is most related to our work in this paper. Here, we review other related work.

*Nonlinear PNC*: In nonlinear PNC systems, the NC mapping at the relay cannot be expressed as a linear weighted sum of the symbols transmitted from the end nodes. A representative work on nonlinear PNC is [12]. Based on an exclusive law to avoid ambiguity in the decoding of NC symbols at the relay, [12] made use of the closest-neighbor clustering principle (corresponding to mapping constellation points of two superimposed symbols separated by  $l_{\min}$  to the same NC symbol in this paper) to map the superimposed symbols of two QPSK symbols of two users to NC symbols in 5QAM constellation at the relay.

Nonlinear PNC mapping based on Latin square was proposed in [13]. Here, the row of the Latin square corresponds to the symbols of one node, and the column represents the symbols of the other node. Entry  $(i, j)$  of the Latin square contains the NC symbol mapped to symbol  $i$  and symbol  $j$  of the two users. The exclusive law of PNC mapping is satisfied by the Latin square's constraint: an NC symbol appears once and only once in each row and in each column. The study of Latin-square nonlinear PNC in [13] focused on low-order  $M$ -PSK (the end nodes transmit  $M$ -PSK signals), and the extension to high-order modulations requires high-order Latin squares. By contrast, as we will show, our Gaussian-integer formulation for linear PNC mapping is scalable with the NC operation with various high-order modulations such as  $q$ -PAM in [9]–[11] and complex modulations in this paper. In particular, for higher-order modulations, the Gaussian-integer formulation only requires selecting the optimal coefficients  $(\alpha, \beta)$  among a larger set of non-zero Gaussian integers.

As far as we know, how to analyze the minimum distances that characterize the decoding performance of  $w_N$  (i.e., what is referred to as  $d_{\min}$  in this paper) is still an open problem for Latin-square nonlinear PNC. For complex linear PNC, on the other hand, as will be shown in this paper, we can explicitly formulate the optimal NC mapping for arbitrary channel gains and characterize the associated minimum distances. Specifically, our paper makes use a Voronoi-region analysis to characterize the optimal NC mapping, and in doing so, we find a systematic approach to identify the minimum distances that affect decoding performance of  $w_N$ .

*Channel-Coded Linear PNC*: In channel-coded linear PNC systems, the two end nodes employ channel coding to encode the transmitted symbols to improve communication reliability. In general, channel-coded PNC can operate in two different

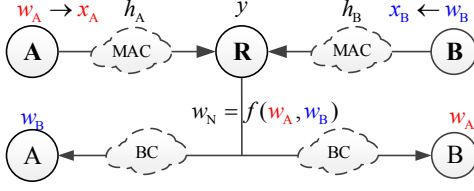


Fig. 1. System model of a TWRN.

ways: link-by-link or end-to-end. For end-to-end channel-coded PNC, the relay is oblivious of the channel coding employed by the two end nodes, and the PNC mapping at the relay is the same as that for nonchannel-coded PNC. Specifically, the relay applies PNC mapping on a symbol-by-symbol basis in both cases. It is at the end nodes after self-information is removed that channel decoding is performed.

For link-by-link channel-coded PNC, the relay is aware of the channel coding employed by the two end nodes (specifically, the relay knows the codebooks used by the two end nodes), and the relay can exploit the correlations among the symbols within each of the channel-coded packets to further improve the accuracy of PNC decoding/mapping. The study of channel-coded PNC systems also originated from low-order modulations such as BPSK [4], [5], and then evolved to high-order modulations in search of higher throughput in the high SNR regime [8], [14]–[19].

The linear PNC studied in this paper falls into class of nonchannel-coded PNC, and it can be naturally integrated into end-to-end channel-coded PNC. Compared with link-by-link channel-coded PNC, end-to-end channel-coded PNC is simpler to operate, at the expense of performance.

### III. COMPLEX LINEAR PNC IN $\mathbb{Z}[i]/q$

#### A. Choosing Representative Elements of $\mathbb{Z}[i]/q$ as Transmitted Symbols

Fig. 1 shows a two-way relay network (TWRN) where nodes A and B communicate with each other via a relay R. In our system model, all nodes (A, B, and R) operate in the half-duplex mode, and each node has single antenna. We assume that there is no direct link between nodes A and B.

Nodes A and B send complex symbols,  $w_A$  and  $w_B$ , simultaneously to relay R. We assume that  $w_A$  and  $w_B$  is selected from  $\mathbb{Z}[i]/q$  (i.e., modulo  $q$  in Gaussian integers), where  $q$  is a Gaussian prime. Note that  $q$  can be complex and that a real prime integer may not be a Gaussian prime [20]. Given prime  $q$ ,  $\mathbb{Z}[i]/q$  is therefore a finite field of order  $|q|^2$ . If  $q$  happens to be also a prime integer (i.e.,  $q = 3 \pmod{4}$ ), then  $\mathbb{Z}[i]/q = \{a + bi | a, b \in \{\frac{1-q}{2}, \dots, 0, \dots, \frac{q-1}{2}\}\}$ . An example of a complex  $q$  is  $q = 1 + 2i$ , for which  $\mathbb{Z}[i]/q \in \{-1, 1, 0, i, -i\}$ . Formally, for arbitrary Gaussian prime  $q$ , we identify the elements in  $\mathbb{Z}[i]/q$  as follows (note: the physical meaning of the Definition 1 will be clearer if the reader refers to the two illustrating examples in Fig. 2 for  $q = 4 + i$  and  $q = 3$  while reading the definition):

**Definition 1** (Residue field of  $\mathbb{Z}[i]/q$ ,  $|q| \geq \sqrt{5}$ ): To identify a set of representative elements of the residue field of  $\mathbb{Z}[i]/q$  when  $|q| \geq \sqrt{5}$ , we set up a coordinate system on the

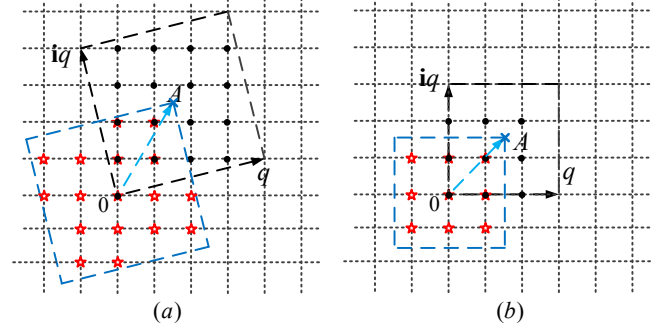


Fig. 2. The congruence class of  $\mathbb{Z}[i]/q$  with (a)  $q = 4 + i$  (b)  $q = 3$ , where red stars are the representative elements of  $\mathbb{Z}[i]/q$  by Definition 1, and black dots within the square formed by  $q$  and  $iq$  are a congruence class of  $\mathbb{Z}[i]/q$ .

2-D complex plane with the basis  $(x, y) = (x^R + x^I i, y^R + y^I i) = (\frac{q}{|q|}, \frac{q}{|q|} i)$ . Given a Gaussian integer  $w = w^R + i w^I \in \mathbb{Z}[i]$  with basis  $(1, i)$ , we define a new coordinate system of  $w$  with the basis  $(x, y) = (\frac{q}{|q|}, \frac{q}{|q|} i)$  as follows:

$$\begin{aligned} w^x &= w^R x^R + w^I x^I, \\ w^y &= w^R y^R + w^I y^I = -w^R x^I + w^I x^R. \end{aligned} \quad (1)$$

To be concise, we rewrite (1) as

$$\begin{bmatrix} w^x \\ w^y \end{bmatrix} = \begin{bmatrix} x^R & x^I \\ -x^I & x^R \end{bmatrix} \begin{bmatrix} w^R \\ w^I \end{bmatrix} = \frac{1}{|q|} \begin{bmatrix} q^R & q^I \\ -q^I & q^R \end{bmatrix} \begin{bmatrix} w^R \\ w^I \end{bmatrix}. \quad (2)$$

We say that  $w \in \mathbb{Z}[i]/q$  if and only if  $|w^x|, |w^y| < |q|/2$  in the new coordinate system. In the context of our communication system model, such a  $w$  is said to be a *valid* symbol.

**Remark 1:** For  $|q| < \sqrt{5}$ , the only possible Gaussian prime  $q$  is  $|q| = \sqrt{2}$ , for which the only possible  $q$  are  $\{1 + i, 1 - i, -1 - i, -1 + i\}$ . Definition 1 above applies to finding the representative elements in  $\mathbb{Z}[i]/q$  with  $|q| = \sqrt{2}$ . For  $|q| = \sqrt{2}$ , we will let the representative elements be  $\{0, 1\}$ . In general, the number of representative elements in  $\mathbb{Z}[i]/q$  is  $|q|^2$  for all  $q$ .

Note that if  $q$  is real (e.g., in Fig. 2(b),  $q = 3$  corresponds to this case), then the basis  $(x, y)$  remains the same as the original basis  $(1, i)$ , since  $x^I = y^R = 0$ , and  $w^x = w^R, w^y = w^I$ . In other words, in the real  $q$  case, the basis consists of the unit vector along the real line and the unit vector along the imaginary line. If  $q$  is complex (e.g., in Fig. 2(a),  $q = 4 + i$  corresponds to this case), the new basis  $(x, y)$  is a rotation of  $(1, i)$  according to  $q$ . Whether  $q$  is real or complex, we require the magnitude of  $w^x$  and  $w^y$  to be strictly less than  $|q|/2$  (for  $|q| \geq \sqrt{5}$ ). With reference to the two illustrating examples in Fig. 2, this means the representative elements must be within the prescribed squares centered around the origin (i.e., the red lattice points). Mathematically, this set of representative elements of  $\mathbb{Z}[i]/q$  is not the only choice. Since congruence modulo  $q$  is an equivalence relation, any  $|q|^2$  elements selected from the  $|q|^2$  congruence classes can be used to represent  $\mathbb{Z}[i]/q$  [20]. In this paper, we choose

the representative elements of  $\mathbb{Z}[i]/q$  by *Definition 1* to serve as the transmitted symbols in our communications systems, since each of such a representative element is the element with the smallest magnitude within its congruence class (i.e., the transmitted power of the corresponding symbol is the smallest). In particular, our definition requires an element of  $\mathbb{Z}[i]/q$  to lie within the zero-centered square of side length  $|q|$  with orientation aligned with the directions as indicated by the basis  $(x, y)$ .

*Proposition 1:* Consider a Gaussian prime  $q$  that defines the valid symbols in  $\mathbb{Z}[i]/q$  by *Definition 1*, where  $|q| \geq \sqrt{5}$ . A sufficient condition for  $w \in \mathbb{Z}[i]/q$  is  $|w| < |q|/2$ .

*Proof of Proposition 1:* Consider the basis  $(x, y)$  in *Definition 1*, we have

$$|w| = \sqrt{(w^R)^2 + (w^I)^2} = \sqrt{(w^x)^2 + (w^y)^2} < |q|/2, \quad (3)$$

since norms are invariant under basis transformation. This implies  $|w^x|, |w^y| < |q|/2$ . Therefore, by *Definition 1*, if  $w \in \mathbb{Z}[i]/q$  if  $|w| < |q|/2$ . ■

At node  $m$ ,  $m \in \{A, B\}$ , a modulated symbol  $x_m$  is given by  $x_m = w_m/\mu$ , where  $\mu$  is a power normalization constant such that  $E(|x_m|^2) = 1$ . If the Gaussian prime  $q$  is a prime integer, the bijective mapping from  $w_m$  to  $x_m$  is equivalent to  $q^2$ -level quadrature amplitude modulation (QAM).

With respect to the TWRN system model shown in Fig. 1, in the MAC phase, nodes A and B transmit  $x_A$  and  $x_B$  simultaneously. At relay R, we assume that the arrival times of the symbols from nodes A and B are aligned, so that the received signal at the relay is given by

$$\begin{aligned} y_R &= h_A \sqrt{P} x_A + h_B \sqrt{P} x_B + z \\ &= \frac{\sqrt{P}}{\mu} (h_A w_A + h_B w_B) + z, \end{aligned} \quad (4)$$

where  $h_m$  is the complex channel coefficient between node  $m$ ,  $m \in \{A, B\}$ , and the relay; and  $z$  is a complex additive white Gaussian noise with zero mean and variance of  $\sigma^2 = N_0$ . We assume  $h_A$  and  $h_B$  are available at relay R, but not at nodes A and B. In addition, nodes A and B transmit with equal power  $P$ .

### B. General Idea of Complex Linear PNC

Upon receiving  $y$ , relay R adopts a linear PNC strategy that tries to derive a network-coded symbol from  $y$ . To understand the details, let us first imagine that  $(w_A, w_B)$  were perfectly known to relay R. Relay R then encodes  $(w_A, w_B)$  to a complex network-coded symbol. We refer to  $(w_A, w_B)$  as a joint symbol. The overall set of joint symbols is  $\mathcal{W}_{(A,B)} = \{(w_A, w_B) | w_A, w_B \in \mathbb{Z}[i]/q\}$ , and  $|\mathcal{W}_{(A,B)}| = |q|^4$ .

Under linear network coding, a joint symbol  $(w_A, w_B) \in \mathcal{W}_{(A,B)}$  is mapped to an NC symbol:

$$w_N^{(\alpha, \beta)} \triangleq f_N^{(\alpha, \beta)}(w_A, w_B) \triangleq \alpha w_A + \beta w_B \pmod{q}, \quad (5)$$

where  $(w_A, w_B) \in \mathbb{Z}[i]/q$ ,  $\alpha, \beta \in \mathbb{Z}[i]/q \setminus \{0\}$ . In this paper, we mark equations in which the multiplications and additions are finite-field operations in  $\mathbb{Z}[i]/q$  by putting the notation

$(\text{mod } q)$  right after the equations, such as in (5). For equations in which the multiplications and additions are not finite-field operations, there will be no  $(\text{mod } q)$  after the equations. Since the NC mapping of (5) is operated in  $\mathbb{Z}[i]/q$ , we refer to it as the *Gaussian-integer formulation*. The advantage of Gaussian-integer formulation over the vector formulation in [10] will be elaborated in Section IV.

In (5), since the field  $\mathbb{Z}[i]/q$  is closed under addition and multiplication,  $w_N^{(\alpha, \beta)} \in \mathbb{Z}[i]/q$ . We refer to  $\alpha, \beta$  as the NC mapping coefficients. We denote the set of all possible NC symbols  $w_N^{(\alpha, \beta)}$  by  $\mathcal{W}_N^{(\alpha, \beta)}$ . Given that  $w_A, w_B \in \mathbb{Z}[i]/q$ , it is easy to see from (5) that  $\mathcal{W}_N^{(\alpha, \beta)} = \mathbb{Z}[i]/q$ , and that  $|\mathcal{W}_N^{(\alpha, \beta)}| = |q|^2$ .

Now, in the actual system, what is known to relay R is  $y$  (which includes the noise  $z$ ) and not the joint symbol  $(w_A, w_B)$ . Conceptually, the decoding process at relay R can be thought of as a two-step process. The first step consists of finding the most likely joint symbol  $(w_A, w_B)$  from  $y$ . The second step consists of the NC mapping as expressed in (5). Note that the decoded  $w_N^{(\alpha, \beta)}$  can still be correct even if the decoding of  $(w_A, w_B)$  is wrong. Specifically, let  $(w_A, w_B)$  be the actual transmitted joint symbols by nodes A and B, and let  $(w'_A, w'_B)$  be the decoded joint symbol. As long as  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$ , the decoded NC symbol  $w_N^{(\alpha, \beta)}$  is still correct. Thus, in general, the decoding error rate of  $w_N^{(\alpha, \beta)}$  is smaller than that of  $(w_A, w_B)$ . The goal of relay R is to find the NC coefficients  $(\alpha, \beta)$  that minimize the decoding error rate of  $w_N^{(\alpha, \beta)}$ .

Returning to Fig. 1, in the BC phase, relay R broadcasts the decoded  $w_N^{(\alpha, \beta)}$  to nodes A and B. If the decoding of  $w_N^{(\alpha, \beta)}$  at the relay is correct and the transmission of  $w_N^{(\alpha, \beta)}$  in the broadcast phase is error-free, then node A can recover the message  $w_B$  with the knowledge of  $(\alpha, \beta)$ , as follows:

$$\beta^{-1}(w_N^{(\alpha, \beta)} - \alpha w_A) = \beta^{-1} \beta w_B = w_B \pmod{q}, \quad (6)$$

where  $\beta^{-1}$  is the multiplicative inverse of  $\beta$  in  $\mathbb{Z}[i]/q$ , i.e.  $\beta^{-1} \beta = 1 \pmod{q}$ . Note that the inverse  $\beta^{-1}$  for the nonzero  $\beta$  exists since  $\mathbb{Z}[i]/q$  is a field. Similarly, node B can recover  $w_A$  if  $\alpha^{-1}$  exists in  $\mathbb{Z}[i]/q$ . The recovery of  $w_m$  at each node is feasible if and only if both  $\alpha$  and  $\beta$  are nonzero in  $\mathbb{Z}[i]/q$ . As long as  $q$  is a Gaussian prime (and therefore  $\mathbb{Z}[i]/q$  is a field), the complex NC mapping under nonzero  $\alpha$  and  $\beta$  is *valid*, in the sense that node A (B) can recover  $w_B$  ( $w_A$ ) using  $w_N^{(\alpha, \beta)}$  and  $w_A$  ( $w_B$ ).

Consider two distinct joint symbols  $(w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A,B)}$ . The difference between these two distinct joint symbols is defined to be

$$(\delta_A, \delta_B) \triangleq (w_A, w_B) - (w'_A, w'_B). \quad (7)$$

We refer to such a  $(\delta_A, \delta_B)$  as a *difference pair*. Note that (7) is not a finite-field equation: the regular integer subtraction is involved, not the finite-field subtraction. We define the set that collects all possible  $(\delta_A, \delta_B)$  induced by two distinct joint symbols in  $\mathcal{W}_{(A,B)}$ , as follows:

$$\Delta \triangleq \{(\delta_A, \delta_B) | (\delta_A, \delta_B) = (w_A, w_B) - (w'_A, w'_B), (w_A, w_B) \neq (w'_A, w'_B), (w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A,B)}\}. \quad (8)$$

Note that unlike  $w_A$  and  $w_B$ ,  $\delta_A, \delta_B$  may not be elements of  $\mathbb{Z}[i]/q$  although their possible values depend on  $\mathbb{Z}[i]/q$ .

We also refer to  $\delta_A$  or  $\delta_B$  as a *difference*. With respect to  $\Delta$ , we define the set that collects all possible  $\delta_A$  or  $\delta_B$  as  $\Lambda$ . Note that the element in  $\Lambda$  can be zero.

Given  $(\delta_A, \delta_B) \in \Delta$ , we define the associated mod- $q$  difference pair as follows:

$$(\delta_A^{(q)}, \delta_B^{(q)}) \triangleq (\delta_A \pmod{q}, \delta_B \pmod{q}), \quad (9)$$

where  $(\delta_A^{(q)}, \delta_B^{(q)}) \in \mathbb{Z}^2[i]/q$  (e.g., if  $(\delta_A, \delta_B) = (8, 9i)$ , then the corresponding  $(\delta_A^{(7)}, \delta_B^{(7)}) = (1, 2i)$ ).

**Proposition 2:** An NC mapping  $f_N^{(\alpha, \beta)}(w_A, w_B)$  maps two distinct joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  in  $\mathcal{W}_{(A, B)}$  to the same NC symbol if and only if  $\alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}$ .

*Proof of Proposition 2:* An NC mapping under  $(\alpha, \beta)$  maps  $(w_A, w_B)$  and  $(w'_A, w'_B)$  to the same NC symbol if and only if  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$ . Thus,

$$\alpha w_A + \beta w_B = \alpha w'_A + \beta w'_B \pmod{q}. \quad (10)$$

Equivalently, we can rewrite (10) as

$$\alpha(w_A - w'_A) + \beta(w_B - w'_B) = \alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}. \quad (11)$$

In this paper, an NC mapping  $(\alpha, \beta)$  is said to *cluster*  $(\delta_A, \delta_B)$  if and only if  $\alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}$ , where  $\delta_A^{(q)} = \delta_A \pmod{q}$  and  $\delta_B^{(q)} = \delta_B \pmod{q}$ . This is a quick way of saying  $(\alpha, \beta)$  map any two joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  satisfying  $(\delta_A^{(q)}, \delta_B^{(q)}) = (w_A, w_B) - (w'_A, w'_B) \pmod{q}$  to the same NC symbol.

**Proposition 3:** Consider two distinct joint symbols  $(w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A, B)}$ . Suppose that we want to find an NC mapping  $f_N^{(\alpha, \beta)}$  such that  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$ . Then, such an NC mapping exists if and only if  $w_A \neq w'_A$  and  $w_B \neq w'_B$ .

*Proof of Proposition 3:* Since  $(w_A, w_B)$  and  $(w'_A, w'_B)$  are distinct, we cannot have  $w_A = w'_A$  and  $w_B = w'_B$  at the same time. Without loss of generality (w.l.o.g.), we will show that an NC mapping with  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$  is not possible if  $w_A = w'_A$  and  $w_B \neq w'_B$ , and is possible if  $w_A \neq w'_A$  and  $w_B \neq w'_B$ .

If  $w_A = w'_A$  and  $w_B \neq w'_B$ , we have  $\delta_A = 0$  and  $\delta_B \neq 0$ . Suppose that  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$  were possible. Then by Proposition 2, we have  $\beta\delta_B^{(q)} = 0 \pmod{q}$ . Since  $\beta \in \mathbb{Z}[i]/q \setminus \{0\}$ , there exists  $\beta^{-1}$  such that  $\beta^{-1}\beta\delta_B^{(q)} = \delta_B^{(q)} = 0 \pmod{q}$ . That is,  $\delta_B = uq$  for some  $u \in \mathbb{Z}[i]$ . According to Definition 1, we have  $\delta_B = [\frac{w_A - w'_A}{|q|} + i\frac{w_A^y - w'_A^y}{|q|}]q$  and  $|w_A^x|, |w_A^y|, |w'_A^x|, |w'_A^y| < |q|/2$ . Thus,  $\frac{w_A^x - w'_A^x}{|q|}$  and  $\frac{w_A^y - w'_A^y}{|q|}$  cannot be non-zero integers and the only possibility for  $u$  is  $u = 0$ . That is,  $\delta_B = 0$ , contradicting the supposition that  $w_B \neq w'_B$ . Thus, an NC mapping is not possible when  $(w_A, w_B)$  and  $(w'_A, w'_B)$  are distinct and  $w_A = w'_A$ .

Next, we prove that we can find  $(\alpha, \beta)$  such that  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$  if  $w_A \neq w'_A$  and  $w_B \neq w'_B$ . In this case,  $\delta_A^{(q)}, \delta_B^{(q)} \neq 0 \pmod{q}$ . This means the

inverses  $(\delta_A^{(q)})^{-1}$  and  $(\delta_B^{(q)})^{-1}$  exist if  $q$  is a Gaussian prime. We need to find a pair,  $\alpha, \beta \neq 0 \pmod{q}$ , such that  $\alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}$ . A possible pair is  $(\alpha, \beta) = (-\delta_A^{(q)})^{-1}\delta_B^{(q)}, 1 \pmod{q}$ .

Motivated by Proposition 3, the definition below specifies a difference pair of two joint symbols that can be mapped to the same NC symbol by NC mapping:

**Definition 2 (NC-validity of  $(\delta_A, \delta_B)$ ):** A difference pair  $(\delta_A, \delta_B)$  is said to be an *NC-valid difference pair* if and only if (1)  $(\delta_A, \delta_B) \in \Delta$  and (2)  $\delta_A \neq 0, \delta_B \neq 0$ . That is,  $(\delta_A, \delta_B)$  is NC-valid only if there is an NC mapping  $(\alpha, \beta)$  that maps two distinct joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  separated by  $(\delta_A, \delta_B)$  to the same NC symbol.

**Definition 3 (Isomorphism of NC mappings):** Two NC mappings  $f_N^{(\alpha, \beta)} : \mathcal{W}_{(A, B)} \rightarrow \mathcal{W}_N^{(\alpha, \beta)}$  and  $f_N^{(\alpha', \beta')} : \mathcal{W}_{(A, B)} \rightarrow \mathcal{W}_N^{(\alpha', \beta')}$  are said to be *isomorphic* if for any two distinct joint symbols  $(w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A, B)}$ ,  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$  if and only if  $f_N^{(\alpha', \beta')}(w_A, w_B) = f_N^{(\alpha', \beta')}(w'_A, w'_B)$ .

Given an NC mapping  $f_N^{(\alpha, \beta)}$ , we can always find another NC mapping isomorphic to  $f_N^{(\alpha, \beta)}$  with a simpler expression, as stated in Proposition 4 below.

**Proposition 4:** Given any NC mapping  $f_N^{(\alpha, \beta)} : \mathcal{W}_{(A, B)} \rightarrow \mathcal{W}_N^{(\alpha, \beta)}$  of the form  $f_N^{(\alpha, \beta)}(w_A, w_B) = \alpha w_A + \beta w_B \pmod{q}$  with  $\beta \in \mathbb{Z}[i]/q \setminus \{0\}$ , the NC mapping  $f_N^{(\alpha', 1)} : \mathcal{W}_{(A, B)} \rightarrow \mathcal{W}_N^{(\alpha', 1)}$ , where  $\alpha' = \beta^{-1}\alpha \pmod{q}$ , is an isomorphic NC mapping.

*Proof of Proposition 4:* Since  $\beta \neq 0$ ,  $\beta^{-1}$  exists. We have

$$\begin{aligned} \beta^{-1}f_N^{(\alpha, \beta)}(w_A, w_B) &= \beta^{-1}(\alpha w_A + \beta w_B) \\ &= \beta^{-1}\alpha w_A + w_B = f_N^{(\alpha', 1)}(w_A, w_B) \pmod{q}. \end{aligned} \quad (12)$$

From (12), since  $\beta^{-1}$  is non-zero, we can see that for two distinct  $(w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A, B)}$ ,  $f_N^{(\alpha, \beta)}(w_A, w_B) = f_N^{(\alpha, \beta)}(w'_A, w'_B)$  if and only if  $f_N^{(\alpha', 1)}(w_A, w_B) = f_N^{(\alpha', 1)}(w'_A, w'_B)$ .

**Definition 4 (Clustered difference pairs):** We refer to the set of NC-valid  $(\delta_A, \delta_B)$  clustered by  $(\alpha, \beta)$  as its *clustered-difference set*:

$$\begin{aligned} \Delta_{(\alpha, \beta)} &= \{(\delta_A, \delta_B) \in \Delta \mid \\ &\alpha(\delta_A \pmod{q}) + \beta(\delta_B \pmod{q}) = 0 \pmod{q}\}. \end{aligned} \quad (13)$$

We refer to the elements in  $\Delta_{(\alpha, \beta)}$  as the *clustered difference pairs*.

The significance of studying  $\Delta_{(\alpha, \beta)}$  lies in that two joint symbols,  $(w_A, w_B)$  and  $(w'_A, w'_B)$ , separated by the clustered difference pair  $(\delta_A, \delta_B) \in \Delta_{(\alpha, \beta)}$  will be mapped to the same NC symbol under  $(\alpha, \beta)$ .

In Appendix I, we use coset theory to interpret the linear PNC mapping in  $\mathbb{Z}[i]/q$ , uncovering the structure of the

isomorphism among different possible PNC mappings  $(\alpha, \beta)$ . The isomorphism substantially reduces the search space of  $(\alpha, \beta)$  when we look for the optimal PNC mapping.

Appendix I further deduces that the complex NC mapping  $f_N^{(\alpha, \beta)} : \mathcal{W}_{(A, B)} \rightarrow \mathcal{W}_N^{(\alpha, \beta)}$  is a  $|q|^2$ -to-1 mapping. This NC mapping partitions  $\mathcal{W}_{(A, B)}$  into  $|q|^2$  subsets (i.e.,  $|q|^2$  cosets), each corresponding to a unique NC symbol, as follows:

$$\mathcal{W}_{(A, B)}(w_N^{(\alpha, \beta)}) \triangleq \{(w_A, w_B) \in \mathbb{Z}^2[i]/q \mid w_N^{(\alpha, \beta)} = f_N^{(\alpha, \beta)}(w_A, w_B)\}. \quad (14)$$

We refer to the partitioning of  $\mathcal{W}_{(A, B)}$  into  $|q|^2$  subsets, each with  $|q|^2$  elements, as the *NC partitioning* under  $(\alpha, \beta)$ .

### C. Distance Metrics of Superimposed Constellation at Relay

Given a pair of  $h_A$  and  $h_B$ , we define a superimposed symbol as

$$w_S \triangleq f_S(w_A, w_B) \triangleq h_A w_A + h_B w_B. \quad (15)$$

Furthermore, we refer to the set of all possible  $w_S$  as  $\mathcal{W}_S$ . Since  $h_A$  and  $h_B$  are selected from the set of all complex numbers,  $\mathcal{W}_S \subset \mathbb{C}$ .

Each joint symbol  $(w_A, w_B) \in \mathcal{W}_{(A, B)}$  corresponds to a superimposed symbol  $w_S$ . Therefore, an NC mapping  $f_N^{(\alpha, \beta)}$  also partitions  $\mathcal{W}_S$  into  $|q|^2$  subsets, each subset being labeled by a specific  $w_N^{(\alpha, \beta)}$  (i.e., elements in a subset are mapped to the same NC symbol). The subset of  $\mathcal{W}_S$  associated with a particular NC symbol  $w_N^{(\alpha, \beta)}$  can be written as

$$\mathcal{W}_S(w_N^{(\alpha, \beta)}) \triangleq \{w_S \in \mathcal{W}_S \mid \exists (w_A, w_B) \in \mathcal{W}_{(A, B)} : w_N^{(\alpha, \beta)} = f_N^{(\alpha, \beta)}(w_A, w_B) \text{ and } w_S = f_S(w_A, w_B)\}. \quad (16)$$

In the constellation of  $\mathcal{W}_S$ , the Euclidean distance between any two superimposed symbols  $w_S$  and  $w'_S$  associated with two distinct joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  is given by

$$l \triangleq |w_S - w'_S| = |h_A \delta_A + h_B \delta_B|. \quad (17)$$

We remark that for a particular  $(\delta_A, \delta_B)$ ,  $(\epsilon \delta_A, \epsilon \delta_B)$  with  $\epsilon \in \{-1, \pm i\}$  has the same distance as  $(\delta_A, \delta_B)$  (i.e., multiplying both  $\delta_A$  and  $\delta_B$  by a unit does not change the distance).

**Definition 5 (Validity of  $\delta_A$  or  $\delta_B$ ):**  $\delta_A$  or  $\delta_B$  is said to be a *valid difference* if and only if  $\delta_A$  or  $\delta_B \in \Delta$ .

**Definition 6 (Distance validity of  $(\delta_A, \delta_B)$ ):**  $(\delta_A, \delta_B)$  is said to be a *distance-valid difference pair* if and only if  $(\delta_A, \delta_B) \in \Delta$ .

**Remark 2:** Note that for  $(\delta_A, \delta_B)$  to be NC-valid, according to Definition 2, we need both  $\delta_A \neq 0$  and  $\delta_B \neq 0$  (i.e.,  $(\delta_A, \delta_B)$  is the difference of two distinct joint symbols that can be mapped to the same NC symbol). On the other hand, for  $(\delta_A, \delta_B)$  to be distance-valid, we only need  $\delta_A \neq 0$  or  $\delta_B \neq 0$  (i.e.,  $(\delta_A, \delta_B)$  corresponds to the difference of two distinct joint symbols, and it makes sense to talk about the distance between the corresponding two superimposed symbols given by (17)). Thus, the set of distance-valid difference pairs is a strict superset of the set of NC-valid difference pairs. The elements that are in the former but not in the latter are those in the former with either  $\delta_A = 0$  or  $\delta_B = 0$ .

Two distance metrics relevant to decoding errors are defined as follows [10], [11]:

- *Minimum symbol distance*  $l_{\min}$

$$l_{\min} \triangleq \arg \min_{\substack{(w_A, w_B) \neq (w'_A, w'_B), \\ (w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A, B)}, \\ w_S = f_S(w_A, w_B), w'_S = f_S(w'_A, w'_B)}} |w_S - w'_S|. \quad (18)$$

- *Minimum NC-symbol distance*  $d_{\min}^{(\alpha, \beta)}$

$$d_{\min}^{(\alpha, \beta)} \triangleq \arg \min_{\substack{(w_A, w_B) \neq (w'_A, w'_B), \\ (w_A, w_B), (w'_A, w'_B) \in \mathcal{W}_{(A, B)}, \\ w_S = f_S(w_A, w_B), w'_S = f_S(w'_A, w'_B), \\ f_N^{(\alpha, \beta)}(w_A, w_B) \neq f_N^{(\alpha, \beta)}(w'_A, w'_B)}} |w_S - w'_S|. \quad (19)$$

In other words,  $l_{\min}$  is the minimum distance among all pairs of superimposed symbols  $w_S$  and  $w'_S$  in the superimposed constellation, and it depends on  $h_A$  and  $h_B$  only. On the other hand,  $d_{\min}^{(\alpha, \beta)}$  is the minimum distance among all pairs of superimposed symbols  $w_S$  and  $w'_S$  in the superimposed constellation that belong to different partitions in (16) (i.e., as far as  $d_{\min}^{(\alpha, \beta)}$  is concerned,  $w_S$  and  $w'_S$  must be associated with different NC symbols). We see that  $d_{\min}^{(\alpha, \beta)} \geq l_{\min}$  in general and, unlike  $l_{\min}$ ,  $d_{\min}^{(\alpha, \beta)}$  depends on the NC coefficients  $(\alpha, \beta)$  as well as  $h_A$  and  $h_B$ .

This paper focuses on the use of a minimum NC-symbol distance mapping rule at the relay. In the high SNR regime, the SER of decoding NC symbols at the relay is dominated by  $d_{\min}^{(\alpha, \beta)}$  [10], [11], which in turn depends on the NC coefficients  $(\alpha, \beta)$ . The minimum NC-symbol distance mapping rule, given below, finds the  $(\alpha, \beta)$  that maximizes  $d_{\min}^{(\alpha, \beta)}$  to minimize SER:

$$(\alpha_{\text{opt}}, \beta_{\text{opt}}) = \arg \max_{\alpha, \beta \in \mathbb{Z}[i]/q \setminus \{0\}} d_{\min}^{(\alpha, \beta)}. \quad (20)$$

W.l.o.g., we consider a normalized version of (4) as follows:

$$\frac{y_R}{h_B} = \eta \sqrt{P} x_A + \sqrt{P} x_B + \frac{z}{h_B}, \quad (21)$$

where  $\eta = \frac{h_A}{h_B} \in \mathbb{C}$ . For simplicity, and w.l.o.g., we assume that  $h_B = 1$  and thereby  $\eta = h_A$ . Accordingly, the superimposed symbol in (15) is scaled as  $w_S = \eta w_A + w_B$  and the Euclidean distance in (17) becomes  $l = |\eta \delta_A + \delta_B|$ .

As an illustrating example, let us consider the case of  $q = 2 + i$  and  $\eta = 1.1 + i$ . When  $q = 2 + i$ , according to Definition 1,  $w_A, w_B \in \mathbb{Z}[i]/(2 + i) = \{0, \pm 1, \pm i\}$ . To see the effect of  $(\alpha, \beta)$  on  $l_{\min}$  and  $d_{\min}^{(\alpha, \beta)}$ , we plot the constellations of the superimposed symbols based on different  $(\alpha, \beta)$  in Fig. 3. In Fig. 3, we use different shapes to label the superimposed symbols mapped to distinct NC symbols; the superimposed symbols with the same shape are mapped to the same NC symbol under the particular  $(\alpha, \beta)$ . In Fig. 3(a),  $(\alpha, \beta) = (1, -i)$ ; in Fig. 3(b),  $(\alpha, \beta) = (i, -i)$ . We observe that  $d_{\min}^{(\alpha, \beta)}$  varies with different  $(\alpha, \beta)$  while  $l_{\min}$  is constant. In particular,  $d_{\min}^{(i, -i)}$  in Fig. 3(b) is larger than  $d_{\min}^{(1, -i)}$  in Fig. 3(a), thus, the NC mapping under  $(\alpha, \beta) = (i, -i)$  should have a better SER performance than under  $(\alpha, \beta) = (1, -i)$  for the decoding of  $w_N^{(\alpha, \beta)}$  in the high SNR regime.



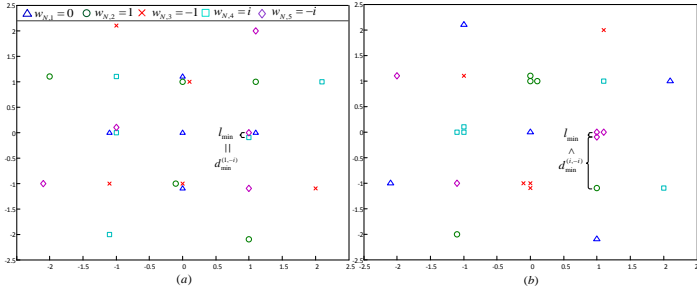


Fig. 3. Constellations of superimposed symbols for complex linear PNC in  $\mathbb{Z}[i]/(2+i)$  when  $(h_A, h_B) = (1.1+i, 1)$  and (a)  $(\alpha, \beta) = (1, -i)$ ; (b)  $(\alpha, \beta) = (i, -i)$ .

The above example illustrates how  $(\alpha, \beta)$  affects  $d_{\min}^{(\alpha, \beta)}$ . This example also brings out two key problems we aim to attack in this paper.

#### Key Problems:

- (1) What is the optimal complex linear PNC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  given  $\eta = h_A/h_B$ ?
- (2) How to characterize  $l_{\min}$  and  $d_{\min}^{(\alpha, \beta)}$  given  $\eta = h_A/h_B$ ?

To address problem (1) in a systematic manner, Section IV will elaborate the advantage of the Gaussian-integer formulation of the complex linear PNC mapping in  $\mathbb{Z}[i]/q$ . In Section V, we will identify the optimal PNC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  for the special  $\eta$  at which  $l_{\min} = 0$  (these  $\eta$  are defined as the zero- $l_{\min}$  channel gains). Section VI then considers the general  $\eta$ . In particular, Section VI shows how to divide the complex plane of  $\eta$  into different Voronoi regions, with an optimal linear PNC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  being associated with each Voronoi region (i.e.,  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  is optimal for  $\eta$  in the Voronoi region).

To address problem (2), Sections V and VI will give systematic approaches to identify  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  at each zero- $l_{\min}$  channel gain and its associated Voronoi region. In particular, in Section VI,  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  for a given  $\eta$  can be derived through a “Voronoi-region analysis”.

#### IV. THE ADVANTAGE OF GAUSSIAN-INTEGER FORMULATION OVER VECTOR FORMULATION

In this section, we elaborate the relationship between the Gaussian-integer formulation and the vector formulation, and show that the Gaussian-integer formulation gives us more choices of linear PNC mappings with a larger set of signal constellations than the vector formulation in [10].

When  $q$  is an prime integer, we can also formulate linear PNC mappings in a vector space in  $GF(q)$ , as in [10]. However, as we will see, this formulation has a limitation when such a prime integer  $q$  is not a Gaussian prime (e.g.,  $q = 2 = (1+i)(1-i)$  is a prime integer, but not a Gaussian prime since it can be factorized)—this is the reason we only consider Gaussian prime  $q$  in this paper. Specifically, in this case, it may not be able to map all the joint symbols separated by the minimum distance  $l_{\min}$  to the same NC symbol when  $l_{\min}$  is very small (including the case where  $\eta$  is such that  $l_{\min} = 0$ ), resulting in small  $d_{\min} = l_{\min}$ .

Overall, this section establishes the following:

- The *equivalence* between the vector formulation in [10] under a “dual mapping” that minimizes  $d_{\min}$  and the Gaussian-integer formulation in this paper when  $q$  is both an integer prime and a Gaussian prime;
- The *limitation* of the vector formulation when  $q$  is an integer prime but not a Gaussian prime.
- The *broader scope* of the Gaussian-integer formulation over the vector formulation when  $q$  is a Gaussian prime but not an integer prime.

The vector mapping scheme of [10] that corresponds to (5) is as follows:

$$\mathbf{w}_N^{(\alpha, \beta)} \triangleq f_N^{(\alpha, \beta)}(\mathbf{w}_A, \mathbf{w}_B) \triangleq \alpha \mathbf{w}_A + \beta \mathbf{w}_B \pmod{q} \quad (22)$$

In the above,  $\alpha = [\alpha_{ij}]_{(2 \times 2)}$  and  $\beta = [\beta_{ij}]_{(2 \times 2)}$ ,  $i, j \in \{1, 2\}$ , are two  $2 \times 2$  NC mapping matrices. The joint symbol and the NC symbol are expressed in vector form as  $(\mathbf{w}_A, \mathbf{w}_B) \triangleq ((w_A^R, w_A^I)^T, (w_B^R, w_B^I)^T)$  and  $w_N^{(\alpha, \beta)} = (w_N^{(\alpha, \beta), R}, w_N^{(\alpha, \beta), I})^T$  respectively, where  $R$  and  $I$  denote the real and imaginary parts of a complex number respectively. In [10], the linear NC mapping in (22) is said to be valid if and only if  $\alpha$  and  $\beta$  are invertible matrices.

Consider two distinct joint symbols  $(\mathbf{w}_A, \mathbf{w}_B)$  and  $(\mathbf{w}'_A, \mathbf{w}'_B)$ . The difference between these two different joints symbols in the vector formulation is  $(\delta_A, \delta_B) \triangleq (\mathbf{w}_A, \mathbf{w}_B) - (\mathbf{w}'_A, \mathbf{w}'_B)$ . Given a prime integer  $q$ ,  $\delta_A^R, \delta_A^I, \delta_B^R, \delta_B^I \in \{-(q-1), \dots, 0, \dots, (q-1)\}$ . The mod- $q$  difference pair is defined as  $(\delta_A^{(q)}, \delta_B^{(q)}) \triangleq (\delta_A \pmod{q}, \delta_B \pmod{q})$ . Given a valid  $(\delta_A, \delta_B)$  in the vector formulation, the associated Gaussian-integer formulation is  $(\delta_A, \delta_B) = (\delta_A^R + i\delta_A^I, \delta_B^R + i\delta_B^I)$ .

- Equivalence under dual mapping when  $q$  is both an integer prime and a Gaussian prime

Consider all  $(\delta_A, \delta_B)$  (or  $(\delta_A, \delta_B)$  in Gaussian integer form) that yields  $l_{\min}$ . To cluster these  $(\delta_A, \delta_B)$ , we show that the NC mapping in the vector formulation under a dual mapping is equivalent to the Gaussian-integer formulation when  $q$ , an integer prime, also happens to be a Gaussian prime.

#### Dual Mapping of Vector Formulation:

For the vector formulation, we define the dual of a particular  $(\delta_A, \delta_B)$  as  $(\bar{\delta}_A, \bar{\delta}_B) \triangleq (-\delta_A^I, \delta_A^R, -\delta_B^I, \delta_B^R)$  [10]. Note that both  $(\delta_A, \delta_B)$  and its dual  $(\bar{\delta}_A, \bar{\delta}_B)$  yield a same distance  $l$ , since  $|h_A(\delta_A^R + i\delta_A^I) + h_B(\delta_B^R + i\delta_B^I)| = |h_A(-\delta_A^I + i\delta_A^R) + h_B(-\delta_B^I + i\delta_B^R)|$ . In other words, under a specific  $\eta$ , if  $(\delta_A, \delta_B)$  yields  $l_{\min}$ , then so does its dual  $(\bar{\delta}_A, \bar{\delta}_B)$ . To maximize  $d_{\min}$ , the NC mapping needs to cluster both  $(\delta_A, \delta_B)$  and its dual  $(\bar{\delta}_A, \bar{\delta}_B)$ . Suppose that this NC mapping is  $(\alpha, \beta) = \left( \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}, \mathbf{I} \right)$  such that

$$\left( \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix}, \mathbf{I} \right) \begin{pmatrix} \delta_A^{R(q)} & -\delta_A^{I(q)} \\ \delta_A^{I(q)} & \delta_A^{R(q)} \\ \delta_B^{R(q)} & -\delta_B^{I(q)} \\ \delta_B^{I(q)} & \delta_B^{R(q)} \end{pmatrix} = \mathbf{0} \pmod{q} \quad (23)$$

where  $\mathbf{I}$  is an identity matrix. For *Proposition 4* in Section III concerning the Gaussian integer formulation, we can find a corresponding *Proposition 4* for the vector formulation. Specifically, for a valid NC mapping where both  $\alpha$  and  $\beta$

are invertible, by isomorphism, we can set  $\beta = \mathbf{I}$  and so that we only need to look for an appropriate  $\alpha$ .

The solution of  $(\alpha, \beta)$  in (23) is given by

$$(\alpha, \beta) = \left( \begin{pmatrix} \alpha^R & -\alpha^I \\ \alpha^I & \alpha^R \end{pmatrix}, \mathbf{I} \right) \quad (24)$$

where

$$\begin{pmatrix} \alpha^R \\ \alpha^I \end{pmatrix} = ((\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2)^{-1} \begin{pmatrix} \delta_A^{R(q)} \delta_B^{R(q)} + \delta_A^{I(q)} \delta_B^{I(q)} \\ \delta_A^{R(q)} \delta_B^{I(q)} - \delta_A^{I(q)} \delta_B^{R(q)} \end{pmatrix} \pmod{q} \quad (25)$$

Note that  $(\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2 \pmod{q}$  is invertible, as explained below. First, the case of  $\delta_A^{R(q)} = \delta_A^{I(q)} = 0$  is eliminated because for an NC-valid  $(\delta_A^{R(q)}, \delta_B^{R(q)})$ , both  $\delta_A^{R(q)}$  and  $\delta_B^{R(q)}$  cannot be zero (see *Definition 2*). W.l.o.g., suppose that  $\delta_A^{I(q)} \neq 0$  and that  $(\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2$  is not invertible (i.e.,  $(\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2 = 0 \pmod{q}$ ). We can write  $((\delta_A^{R(q)})(\delta_A^{I(q)})^{-1})^2 = -1 \pmod{q}$ . However, this contradicts *Lemma 1* below, which states that  $((\delta_A^{R(q)})(\delta_A^{I(q)})^{-1})^2 = -1 \pmod{q}$  has a solution if and only if  $q = 1 \pmod{4}$ ; but the  $q$  being considered here is a prime integer as well as a Gaussian prime, which requires  $q = 3 \pmod{4}$ .

*Lemma 1 (Law of Quadratic Reciprocity):* The congruence  $x^2 = -1 \pmod{q}$  is solvable if and only if  $q = 1 \pmod{4}$  [28].

Furthermore, we can verify that  $(\alpha, \beta)$  in (24) is equivalent to  $(\alpha, \beta) = (\alpha^R + i\alpha^I, 1) = (-(\delta_A^{R(q)})^{-1}\delta_B^{R(q)}, 1)$  in the Gaussian-integer formulation, where  $(\delta_A^{R(q)})^{-1} = ((\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2)^{-1}(\delta_A^{R(q)} + i\delta_A^{I(q)})$ . Therefore, the vector formulation in [10] under the dual mapping is equivalent to the Gaussian-integer formulation in (5) when  $q$  is a prime integer that is also a Gaussian prime.

- Limitation of the vector formulation when  $q$  is an integer prime but not a Gaussian prime.

From our previous discussions in (24), dual mapping under the vector formulation is desired. Otherwise,  $d_{\min} = l_{\min}$  for all  $\eta$  and the system performance will be poor (any arbitrary NC mapping can achieve  $d_{\min} = l_{\min}$  and a system adopting the vector formulation without insisting on dual mapping is an unoptimized systems).

Furthermore, we also know that dual mapping under the vector formulation is always feasible when the integer prime  $q$  also happens to be a Gaussian prime. However, when  $q$  is an integer prime, but not a Gaussian prime, dual mapping may not be possible (specifically, this occurs when  $(\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2 = 0 \pmod{q}$  in (25) so that a nonzero  $\alpha$  is not possible). For the vector formulation, when the dual mapping is not satisfied, we have  $d_{\min} = l_{\min}$ . In the following, we give an example showing that when  $q$  is an integer prime but not a Gaussian prime, and when  $\eta$  is such that  $l_{\min}$  is small, we cannot find an NC mapping in the vector formulation to cluster all  $(\delta_A, \delta_B)$  that yield the same  $l_{\min}$ .

Let us consider  $q = 2$  (i.e., 4QAM), which is an integer prime but not Gaussian prime. Let the four representative elements in  $\mathbb{Z}[i]/2$  be  $\{0, 1, i, 1+i\}$  (note that *Definition 1*

does not apply to  $q = 2$ ). Therefore, for  $q = 2$ , we have  $\delta_A, \delta_B \in \{0, \pm 1, \pm i, \pm(1+i), \pm(1-i)\}$ . At  $\eta = \frac{1+i}{2}$ , we find that  $(\delta_A, \delta_B) = (1, -1, -1, 0)$  and its dual  $(1, 1, 0, -1)$  yield  $l_{\min} = 0$ . Their corresponding mod- $q$  difference pairs are  $(\delta_A^{(q)}, \delta_B^{(q)}) = (1, 1, 1, 0)$  and  $(1, 1, 0, 1)$ . At this  $\eta$ , we cannot find a valid dual mapping, since  $(\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2 = 0 \pmod{2}$  is not invertible in  $GF(2)$ . We can choose to cluster either  $(1, 1, 1, 0)$  or  $(1, 1, 0, 1)$  but not both (i.e., with respect to (23), we could design  $(\alpha_1, \alpha_2)$  to cluster the former, or design  $(\alpha_3, \alpha_4)$  to cluster the latter, but not both at the same time). As a consequence,  $d_{\min} = l_{\min} = 0$ . When  $\eta$  deviates from  $\frac{1+i}{2}$  a little bit so that  $(\delta_A, \delta_B) = (1, -1, -1, 0)$  and its dual  $(1, 1, 0, -1)$  still yield  $l_{\min}$ , but  $l_{\min}$  is slightly larger than 0, the dual mapping cannot be satisfied either. Thus,  $d_{\min} = l_{\min} \approx 0$ . For  $q > 2$ , the same problem arises when  $q$  is an integer prime such that  $q = 1 \pmod{4}$ , i.e., when  $q$  is not a Gaussian prime.

- Broader scope of Gaussian-integer formulation

For good performance, adopting dual mapping under the vector formulation limits us to  $q$  that are prime integers as well as Gaussian primes ( $q = 3, 7, 11, 19, \dots$ ). The Gaussian-integer formulation, on the other hand, can also solve the same dual mapping problem of the vector formulation in more concise way. Going beyond that, the Gaussian-integer formulation allows us to adopt complex  $q$  (not just real  $q$ ) that are Gaussian primes. There are many such complex Gaussian primes (e.g.,  $q = 1+i, 1+2i, \dots$  as listed in Fig. 4).

To deal with these Gaussian primes, Gaussian-integer formulation uses the residues of the associated Gaussian prime field  $\mathbb{Z}[i]/q$  as the signal constellation (modulation) used by nodes A and B. The cardinality of such a signal constellation is  $|q|^2$ . Therefore, with Gaussian integer formulation, we have more flexibility than with vector formulation in terms of the choices for signal constellations.

Returning to the example of  $q = 2$ . Both the vector formulation and the Gaussian-integer formulation cannot satisfy the dual mapping requirement at some  $\eta$  when  $l_{\min}$  is very small. The case of  $q = 2$  corresponds to nodes A and B adopting 4-QAM as their signal constellation, for which the number of points on the constellation (the cardinality of the modulation) is 4. If we insist on using an integer  $q$ , the next available constellation is that of  $q = 3$ , with cardinality 9; and after that, that of  $q = 7$ , with cardinality 49. We cannot find a constellation close to the 4-QAM for our purpose.

Complex  $q$  in the Gaussian-integer formulation fills in this gap. Let us consider  $q = 1+2i$  as an example. Under the Gaussian integer formulation, the constellation points (residues of  $\pmod{q}$ , i.e.,  $\mathbb{Z}[i]/(1+2i)$ ) in this case are  $\{0, 1, -1, +i, -i\}$ . The constellation cardinality is 5, closer to the cardinality of  $q = 2$ , which is 4. To be a linear NC mapping in  $\mathbb{Z}[i]/q$ , we require  $\alpha, \beta \in \mathbb{Z}[i]/q \setminus \{0\}$ . With the same channel gain as the  $q = 2$  example above where  $\eta = \frac{1+i}{2}$ , we find that  $(\delta_A, \delta_B) = (1-i, -1)$  and  $(1+i, -i)$  yield  $l_{\min} = 0$ . Recall that when  $q = 2$ , the dual mapping cannot be satisfied under both the vector formulation and Gaussian-integer formulation at this  $\eta$ . However, when  $q = 1+2i$ ,  $(\delta_A^{R(q)})^2 + (\delta_A^{I(q)})^2$  is invertible in  $\mathbb{Z}[i]/(1+2i)$ . By *Proposition 2*, we can easily



$q$	$1+i$	$1+2i$	3	$2+3i$	$1+4i$	$2+5i$	$1+6i$	$4+5i$	7	...
Cardinality of signal constellation	2	5	9	13	17	29	37	41	49	...

(Subcases covered by vector formulation)

Fig. 4. Possible values of  $q$  and the cardinalities of the corresponding signal constellations possible with the Gaussian integer formulation, and the subcases possible with the vector formulation.

verify that the NC mapping with  $\alpha = -1$  and  $\beta = 1$  can cluster the NC-valid  $(\delta_A, \delta_B) = (1-i, -1)$  and  $(1+i, -i)$  together.

Finally, as shown in Fig. 4, if we order the cardinality from small to large, between two real  $q$  that can be used for our purpose, there are many complex  $q$  offering cardinalities in between the cardinalities of the two real  $q$ . In other words, the Gaussian-integer formulation offers us more choices in terms of constellation cardinality than the vector formulation.

#### V. $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ ANALYSIS AT ZERO- $l_{\min}$ CHANNEL GAINS

This section analyzes  $l_{\min}$  as a function of  $\eta$ , and focuses on those special  $\eta$  at which  $l_{\min} = 0$  for the study of optimal NC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  and  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ . Building on the foundation established in this section, Section VI will consider the optimal NC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  and  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  for general  $\eta$ .

Consider a particular valid  $(\delta_A, \delta_B)$ . When  $\eta = -\delta_B/\delta_A$ , we have  $l_{\min} = 0$ , i.e.,  $|\eta\delta_A + \delta_B| = 0$ . We refer to such an  $\eta$  as a *zero- $l_{\min}$  channel gain*. Each distance-valid  $(\delta_A, \delta_B) \in \Delta$  induces a zero- $l_{\min}$  channel gain. Two superimposed symbols separated by  $(\delta_A, \delta_B)$  overlap with each other at the zero- $l_{\min}$  channel gain  $\eta = -\delta_B/\delta_A$ . Note that there could be multiple  $(\delta_A, \delta_B)$  associated with the same  $\eta$ , since  $\eta$  is a ratio of  $-\delta_B$  and  $\delta_A$ . If there is a common factor between  $\delta_A$  and  $\delta_B$ , we could factor out the common factor to find another  $(\delta'_A, \delta'_B)$  and still retain the same  $\eta = -\delta_B/\delta_A = -\delta'_B/\delta'_A$ . In this paper, we refer to the  $(\delta_A, \delta_B)$  with no common factor between  $\delta_A$  and  $\delta_B$  as a *characteristic difference pair* and denote such difference pair by  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ . Note that, strictly speaking, a characteristic difference is actually a difference pair rather than a difference. We opt to use the term “characteristic difference” for simplicity. As will be seen,  $l_{\min}$  and  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  are determined by characteristic differences; non-characteristic differences are not fundamental to the study of  $l_{\min}$  and  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ .

We remark that  $\eta = 0$  and  $\eta = \epsilon \cdot \infty$  are also zero- $l_{\min}$  channel gains ( $\epsilon = 1, -1, i$  or  $-i$  is the unit). The former corresponds to the case where  $\delta_B = 0$  and  $\delta_A \neq 0$ , and the latter corresponds to the case where  $\delta_A = 0$  and  $\delta_B \neq 0$ . The characteristic difference for  $\eta = 0$  is  $(\delta_A, \delta_B) = (\epsilon, 0)$  and the characteristic difference for  $\eta = \epsilon \cdot \infty$  is  $(0, \epsilon)$  (this is the outcome of all Gaussian integers being a factor of 0, and we will see later that it also makes sense for our problem of identifying the minimum distance in this paper). We will refer to  $\eta = 0$  and  $\eta = \epsilon \cdot \infty$  as the trivial zero- $l_{\min}$  channel gains

because communication basically breaks down at this  $\eta$  (e.g., at  $\eta = 0$ ,  $h_A = 0$ ). Also, by *Definition 6*, the distance-valid difference pairs that induce trivial zero- $l_{\min}$  channel gains are not NC-valid and they cannot be clustered by an NC mapping  $(\alpha, \beta)$  (the implication is that, as with  $l_{\min}$ ,  $d_{\min}$  is also 0 at such  $\eta$ —note that this is not unreasonable from an intuitive viewpoint, because we should not expect good communication performance anyway since the channel gain of one node is 0). On the other hands, all non-trivial distance-valid difference pairs are also NC-valid and they can be clustered by an NC mapping (the implication is that at non-trivial zero- $l_{\min}$  channel gains,  $d_{\min} > 0$  at such  $\eta$ ). The notion will be made clear later in this paper.

Before delving into the details, let us review some fundamental definitions of Gaussian integers.

*Definition 7:* The *norm* of a Gaussian integer  $a = a^R + ia^I \in \mathbb{Z}[i]$  is  $|a|^2 = (a^R)^2 + (a^I)^2$ .

*Definition 8:* The *units* of  $\mathbb{Z}[i]$  are those elements with norm 1, i.e., the units are  $1, -1, i, -i$ .

*Definition 9:* Consider  $a, b \in \mathbb{Z}[i]$  where at least one of  $a$  or  $b$  is non-zero. A *greatest common divisor* (gcd) of  $a$  and  $b$ ,  $\text{gcd}(a, b)$ , is a common divisor with maximal norm. Note that  $\text{gcd}(0, a) = a$ , where  $a$  is non-zero.

*Definition 10:* The *associates* of a Gaussian integer  $a$  are  $a, -a, ia$ , and  $-ia$ .

Note that the  $\text{gcd}(a, b)$  is not unique. If  $c$  is a gcd of  $a$  and  $b$ , then so are the associates of  $c$ . This is because the factorization of a Gaussian integers is not unique: a factor and all its associates are all valid factors (e.g., if  $a = cd$  where  $c$  and  $d$  are the factors, then  $a$  can also be written as  $a = (-c)(-d)$ ,  $(ic)(-id)$ , or  $(-ic)(id)$ .)

In this paper, when we say  $\text{gcd}(a, b) = 1$ , we mean the unit associates are the gcd of  $a$  and  $b$ .

*Definition 11:* Consider  $a, b \in \mathbb{Z}[i]$  where at least one of  $a$  or  $b$  is non-zero. Then  $a$  and  $b$  are said to be *coprime* if they only have unit factors in common (i.e.,  $\text{gcd}(a, b) = 1$ ).

#### A. $l_{\min}$ Versus $\eta$ Analysis and Characteristic Difference

Before analyzing zero- $l_{\min}$  channel gains in detail, let us first quickly show how  $l_{\min}$  varies as a function of  $\eta$ . As defined in (17), the distance  $l$  induced by a distance-valid  $(\delta_A, \delta_B)$  at a particular  $\eta$  (i.e., this is the distance between two superimposed symbols separated by  $(\delta_A, \delta_B)$ ) is given by

$$l_{(\delta_A, \delta_B)}(\eta) \triangleq |\eta\delta_A + \delta_B|. \quad (26)$$

Let us write the real and imaginary parts of the following variables explicitly:  $\delta_A = \delta_A^R + i\delta_A^I$ ,  $\delta_B = \delta_B^R + i\delta_B^I$ , and  $\eta = \eta^R + i\eta^I$ . We can then rewrite (26) as

$$\begin{aligned} l_{(\delta_A, \delta_B)}^2(\eta) &= (\eta^R\delta_A^R - \eta^I\delta_A^I + \delta_B^R)^2 + (\eta^R\delta_A^I + \eta^I\delta_A^R + \delta_B^I)^2 \\ &= (\eta^R)^2|\delta_A|^2 + 2\eta^R(\delta_A^R\delta_B^R + \delta_A^I\delta_B^I) + (\eta^I)^2|\delta_A|^2 \\ &\quad + 2\eta^I(\delta_A^R\delta_B^I - \delta_A^I\delta_B^R) + |\delta_B|^2, \end{aligned} \quad (27)$$

$$\frac{l_{(\delta_A, \delta_B)}^2(\eta)}{|\delta_A|^2} = (\eta^R + \frac{\delta_A^R\delta_B^R + \delta_A^I\delta_B^I}{|\delta_A|^2})^2 + (\eta^I + \frac{\delta_A^R\delta_B^I - \delta_A^I\delta_B^R}{|\delta_A|^2})^2. \quad (28)$$

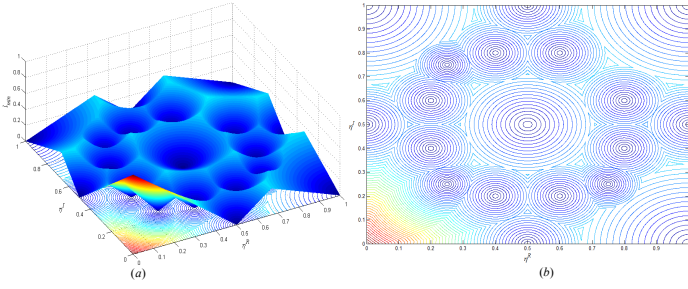


Fig. 5. (a)  $l_{\min}(\eta)$  surface; (b) contour graph of  $l_{\min}(\eta)$ .

or equivalently,

$$\frac{l_{(\delta_A, \delta_B)}(\eta)}{|\delta_A|} = \left| \eta + \frac{\delta_B}{\delta_A} \right|. \quad (29)$$

From (28) (or (29)), we can see that  $l_{(\delta_A, \delta_B)}(\eta)$  as a function of  $\eta$  is a cone with vertex at  $\eta^o \triangleq -\delta_B/\delta_A$ . Following the definition of  $l_{\min}$  in (18), which is the minimum distance among the distances of  $l_{(\delta_A, \delta_B)}(\eta)$  for all distance-valid  $(\delta_A, \delta_B) \in \Delta$ , where  $\Delta$  is defined in (8), we can write

$$l_{\min}(\eta) = \min_{(\delta_A, \delta_B) \in \Delta} l_{(\delta_A, \delta_B)}(\eta). \quad (30)$$

To see how  $l_{\min}(\eta)$  varies with  $\eta$ , we plot a three-dimensional graph of  $l_{\min}(\eta)$  surface in Fig. 5(a) and its contour graph in Fig. 5(b) when  $q = 3$ . We observe that

- $l_{\min}(\eta)$  reaches a minimum value of zero value at the vertices of the cones as defined in (28) for all distance-valid  $(\delta_A, \delta_B) \in \Delta$  (i.e., at zero- $l_{\min}$  channel gains);
- $l_{\min}(\eta)$  reaches a local maximum point at the intersections between three or more adjacent cones, and a “local maximum edge” at the intersections between two adjacent cones (this will be verified in Section VI).

Now, consider a particular cone induced by a particular distance-valid  $(\delta_A, \delta_B)$ . At the vertex of the cone,  $\eta^o = -\delta_B/\delta_A$ , there could be other distance-valid  $(\delta'_A, \delta'_B) \in \Delta$  that also yield  $l_{\min}(\eta^o) = 0$ . In particular, this happens if  $\frac{\delta'_B}{\delta'_A} = \frac{\delta_B}{\delta_A}$ . At this  $\eta^o$ , we define the set that collects all  $(\delta_A, \delta_B) \in \Delta$  that yield  $l_{\min}(\eta^o) = 0$  as follows:

$$\Delta_{\eta^o} \triangleq \{(\delta_A, \delta_B) \in \Delta \mid \eta^o \delta_A + \delta_B = 0\}. \quad (31)$$

**Definition 12 (Characteristic difference):** For a given zero- $l_{\min}$  channel gain  $\eta^o$  and its associated  $\Delta_{\eta^o}$ , we define the characteristic difference  $(\delta_A^{char}, \delta_B^{char})$  as  $(\delta_A, \delta_B)$ :  $\gcd(\delta_A, \delta_B) = 1$ ,  $(\delta_A, \delta_B) \in \Delta_{\eta^o}$ .

**Remark 3:** At a particular  $\eta^o$ , the characteristic difference is unique except for the collection of associates  $(\delta_A, \delta_B) = (\epsilon \delta_A^{char}, \epsilon \delta_B^{char})$  for  $\epsilon \in \{\pm 1, \pm i\}$ .

Each of  $(\delta_A, \delta_B) \in \Delta_{\eta^o}$  induces a cone centered at  $\eta^o$  given by  $l_{(\delta_A, \delta_B)}(\eta) = |\eta \delta_A + \delta_B|$ . Among all the cones,  $(\delta_A^{char}, \delta_B^{char})$  gives the smallest  $l$  for all  $\eta$ , since  $|\eta \delta_A^{char} + \delta_B^{char}| < |\gcd(\delta_A, \delta_B)| |\eta \delta_A^{char} + \delta_B^{char}| = |\eta \delta_A + \delta_B|$ . Thus, as shown in Fig. 5(a),  $l_{\min}$  at  $\eta$  in the neighborhood of  $\eta^o$  is given by the cone of  $l_{(\delta_A^{char}, \delta_B^{char})}(\eta)$ . In particular,  $l_{\min}(\eta)$

can never be given by the cones of non-characteristic  $(\delta_A, \delta_B)$  except at  $\eta^o$ . In studying  $l_{\min}(\eta)$  as a function of  $\eta^o$ , it suffices to restrict our attention to  $(\delta_A^{char}, \delta_B^{char})$ .

Furthermore, consider a cone with vertex  $\eta^o$ . For a fixed value  $l_{(\delta_A, \delta_B)}(\eta)$  of the cone, note from (29) that the contour of  $\eta$  that achieves this fixed  $l_{(\delta_A, \delta_B)}(\eta)$ , is a circle of radius  $\frac{l_{(\delta_A, \delta_B)}}{|\delta_A|}$  centered at  $(-\frac{\delta_A^R \delta_B^I + \delta_A^I \delta_B^R}{|\delta_A|^2}, -\frac{\delta_A^R \delta_B^R - \delta_A^I \delta_B^I}{|\delta_A|^2})$ . Thus, as shown in Fig. 5(b), the contour lines of  $l_{(\delta_A^{char}, \delta_B^{char})}$  for a particular  $(\delta_A^{char}, \delta_B^{char})$  are concentric circles centered at  $(-\frac{\delta_A^{char,R} \delta_B^{char,R} + \delta_A^{char,I} \delta_B^{char,I}}{|\delta_A^{char}|^2}, -\frac{\delta_A^{char,R} \delta_B^{char,I} - \delta_A^{char,I} \delta_B^{char,R}}{|\delta_A^{char}|^2})$ .

For a particular  $q$ , the aforementioned minima and local maxima for  $l_{\min}$  characterize the performance of NC mapping at various  $\eta$ , since post-NC mapping  $d_{\min}^{(\alpha, \beta)}$  is related to  $l_{\min}$ . In Part B below, we first study minima at the zero- $l_{\min}$  channel gains. In Section VI, we will consider the local maxima.

### B. Identifying Zero- $l_{\min}$ Channel Gains and Characteristic Differences

By the definition of zero- $l_{\min}$  channel gain, we can identify all  $\eta$  at which  $l_{\min} = 0$  in the complex plane of  $\eta$  and their associated characteristic differences. To be specific, given a  $q$ , we can go through all  $(\delta_A, \delta_B) \in \Delta$  of (8) to find all  $\eta$  such that  $\eta \delta_A + \delta_B = 0$ . Then, we have a set that collects all distinct zero- $l_{\min}$  channel gains as  $\mathcal{H}^o = \{\eta^o \mid \eta^o = -\delta_B/\delta_A, (\delta_A, \delta_B) \in \Delta\}$ . Then, for each  $\eta^o \in \mathcal{H}^o$ , we select the characteristic difference  $(\delta_A^{char}, \delta_B^{char}) \in \Delta_{\eta^o}$  in (31) by *Definition 12*.

**Remark 4:** The distance-valid difference pairs  $(\delta_A, \delta_B) \in \Delta_{\eta^o}$  where  $\delta_A \neq 0$  and  $\delta_B = 0$  correspond to a *trivial* zero- $l_{\min}$  channel gain  $\eta^o = 0$ . Similarly, we also have a trivial zero- $l_{\min}$  channel gain at  $\eta^o = \infty$ , which is induced by  $\delta_A = 0, \delta_B \neq 0$ . From *Remark 2*, the distance-valid difference pair associated with this trivial zero- $l_{\min}$  channel gain cannot be clustered by any NC mapping. By *Definition 12*, the characteristic difference at the trivial zero- $l_{\min}$  channel  $\eta^o = 0$  is  $(\delta_A^{char}, \delta_B^{char}) = (1, 0)$  and the characteristic difference at the trivial zero- $l_{\min}$  channel  $\eta^o = \infty$  is  $(\delta_A^{char}, \delta_B^{char}) = (0, 1)$ . The distance-valid difference pairs where both  $\delta_A \neq 0$  and  $\delta_B \neq 0$ , i.e., NC-valid difference pairs, correspond to the *non-trivial* zero- $l_{\min}$  channel gains  $\eta^o \neq 0$ .

The proposition below simplifies our search for the zero- $l_{\min}$  channel gains in the complex plane of  $\eta$ , by exploiting a symmetry property.

**Proposition 5 (Zero- $l_{\min}$  symmetry):** Consider a zero- $l_{\min}$  channel gain  $\eta^o = |\eta^o| e^{i\theta^o}$  within  $0 < \theta^o < \pi/4$  in the complex plane of  $\eta$ . Suppose that the characteristic difference at this  $\eta^o$  is  $(\delta_A^{char}, \delta_B^{char})$ . Given this  $\eta^o$ , we can find seven other “symmetric” zero- $l_{\min}$  channel gains in the complex plane of  $\eta$  as follows:

$$\begin{aligned} & |\eta^o| e^{i(\frac{\pi}{2} - \theta^o)}, |\eta^o| e^{i(\frac{\pi}{2} + \theta^o)}, |\eta^o| e^{i(\pi - \theta^o)}, \\ & |\eta^o| e^{i(\pi + \theta^o)}, |\eta^o| e^{i(\frac{3\pi}{2} - \theta^o)}, \\ & |\eta^o| e^{i(\frac{3\pi}{2} + \theta^o)}, \text{ and } |\eta^o| e^{i(2\pi - \theta^o)}. \end{aligned} \quad (32)$$



belong to the clustered-difference set of  $(\alpha, \beta)$ . Therefore, the NC mapping in (34) is optimal for the nontrivial zero- $l_{\min}$  channel gain.

#### D. Identifying $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ at Zero- $l_{\min}$ Channel Gains

In Part B, we have identified all zero- $l_{\min}$  channel gains in the complex plane of  $\eta$  and the associated characteristic differences. In particular, each characteristic difference  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  yields the  $l_{\min}$  at  $\eta$  in the neighborhood of the associated channel gain  $\eta^o$  through the relationship  $l_{\min}(\eta) = \eta \delta_A^{\text{char}} + \delta_B^{\text{char}}$ . Specifically, this  $l_{\min}$  corresponds to a cone centered at  $\eta^o$ , as illustrated in Fig. 5. In this part, we aim to identify  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  at zero- $l_{\min}$  channel gains.

**Trivial Theorem:** At the trivial zero- $l_{\min}$  channel gain  $\eta^o = 0$  and  $\eta^o = \infty$ ,  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})} = l_{\min} = 0$ .

By Remark 2, the characteristic difference  $(\delta_A^{\text{char}}, \delta_B^{\text{char}}) = (1, 0)$  and  $(0, 1)$  associated with the trivial zero- $l_{\min}$  channel gains  $\eta^o = 0$  and  $\eta^o = \infty$  cannot be clustered by any NC mapping. Therefore, at the trivial zero- $l_{\min}$  channel gains,  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})} = l_{\min} = 0$ .

**Theorem 2:** Consider a particular nontrivial zero- $l_{\min}$  channel gain  $\eta^o$  associated with the characteristic difference  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  that can be clustered by the NC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$ . There exists a characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that determines the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  at this  $\eta^o$  such that  $|\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}| = 1$  and that  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})} = |\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| = \frac{1}{|\delta_B^{\text{char}}|}$ .

**Proof of Theorem 2:** Let us assume the validity of the statements of (T2-1) and (T2-2) below. They will be proved separately.

(T2-1) There exists a characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  yielding  $|\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}| = 1$  (in Lemma 6), and

(T2-2) For a  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that satisfies  $|\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}| = 1$ ,  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  and  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  cannot be clustered by the same NC mapping  $(\alpha, \beta)$ .

(T2-1) together with (T2-2) imply  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})} = |\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| = \frac{1}{|\delta_B^{\text{char}}|}$  for the following reason. Given that  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  and  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  cannot be clustered by the same NC mapping, then under the optimal NC mapping that clusters  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  at  $\eta^o = -\delta_B/\delta_A$ ,  $(\alpha_{\text{opt}}, \beta_{\text{opt}}) = (-\delta_B/\delta_A, 1)$ , the distance  $l = |\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}|$  is a potential candidate for  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ . Now,  $|\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| > 0$  for all characteristic differences  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that cannot be clustered by  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$ . This means  $|\delta_A^{\text{char}}||\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| = |\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}| > 0$ . But then  $|\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}|$  must be an integer, meaning  $|\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}| \geq 1$ . Thus,  $|\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| \geq \frac{1}{|\delta_B^{\text{char}}|}$ . Among all  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that cannot be clustered by  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$ ,  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  can meet the lower bound of the inequality: i.e.,  $|\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| = \frac{1}{|\delta_B^{\text{char}}|}$  according to (T2-1) and (T2-2). Thus,  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})} = |\eta^o \delta_A^{\text{char}'} + \delta_B^{\text{char}'}| = \frac{1}{|\delta_B^{\text{char}}|}$ .

**Remark 6:** Note that the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining differences for a given zero- $l_{\min}$  channel gain  $\eta^o = -\delta_B^{\text{char}}/\delta_A^{\text{char}}$  may not be unique, since the characteristic differences that satisfy Theorem 2 may not be unique. For example,  $\eta^o = \frac{1+i}{2}$  in Fig. 5 is associated with the characteristic difference  $(\delta_A^{\text{char}}, \delta_B^{\text{char}}) = (1+i, -i)$ . The multiple  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining differences  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  for this  $\eta^o$  within  $\theta^o \in [0, \pi/4]$  are  $(1+2i, -i)$ ,  $(2+i, -1-i)$ ,  $(2+2i, -1-2i)$ ,  $(1+2i, -2i)$ , and  $(2+i, -1-2i)$ —they all yield  $|\delta_B^{\text{char}} \delta_A^{\text{char}'} - \delta_A^{\text{char}} \delta_B^{\text{char}'}| = 1$ .

The proof of (T2-2) is straightforward and is as follows: A solution for the NC mapping that can cluster  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  is  $(\alpha_{\text{opt}}, \beta_{\text{opt}}) = (-\delta_B^{\text{char}(q)}/\delta_A^{\text{char}(q)}, \delta_A^{\text{char}(q)})$  (other solutions are isomorphic). Suppose that  $(\alpha_{\text{opt}}, \beta_{\text{opt}}) = (-\delta_B^{\text{char}(q)}/\delta_A^{\text{char}(q)}, \delta_A^{\text{char}(q)})$  can also cluster  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$ . Then,  $-\delta_B^{\text{char}(q)}/\delta_A^{\text{char}(q)} \delta_A^{\text{char}'(q)} + \delta_A^{\text{char}(q)} \delta_B^{\text{char}'(q)} = 0 \pmod{q}$ . Therefore,  $\delta_B^{\text{char}(q)} \delta_A^{\text{char}'(q)} - \delta_A^{\text{char}(q)} \delta_B^{\text{char}'(q)} = uq$  for some Gaussian integer  $u$ . Given that  $q$  is not a unit, we must have that  $|\delta_B^{\text{char}(q)} \delta_A^{\text{char}'(q)} - \delta_A^{\text{char}(q)} \delta_B^{\text{char}'(q)}| = |u||q| \neq 1$ , leading to a contradiction. Thus,  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  cannot cluster  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  at the same time.

The proof of (T2-1) is much more involved, and is given through a series of lemmas (Lemmas 2 to 6) in the following. Let us first define a few distance measures to clarify the issue.

Consider two distinct zero- $l_{\min}$  channel gains  $\eta_i^o$  and  $\eta_j^o$  ( $\eta_i^o$  and  $\eta_j^o$  can be trivial or nontrivial zero- $l_{\min}$  channel gains). Suppose that  $(\delta_{A,i}^{\text{char}}, \delta_{B,i}^{\text{char}})$  and  $(\delta_{A,j}^{\text{char}}, \delta_{B,j}^{\text{char}})$  are the two characteristic differences associated with  $\eta_i^o$  and  $\eta_j^o$  respectively. We define the *Euclidean distance*, *normalized distance*, and *weighted distance* between  $\eta_i^o$  and  $\eta_j^o$  as follows:

- The *Euclidean distance* between  $\eta_i^o$  and  $\eta_j^o$

$$d_{ij} \triangleq |\eta_i^o - \eta_j^o| = \left| \frac{\delta_{B,i}^{\text{char}}}{\delta_{A,i}^{\text{char}}} - \frac{\delta_{B,j}^{\text{char}}}{\delta_{A,j}^{\text{char}}} \right| = \frac{|\delta_{B,i}^{\text{char}} \delta_{A,j}^{\text{char}} - \delta_{A,i}^{\text{char}} \delta_{B,j}^{\text{char}}|}{|\delta_{A,i}^{\text{char}}| |\delta_{A,j}^{\text{char}}|} \quad (35)$$

- The *normalized distance* between  $\eta_i^o$  and  $\eta_j^o$

$$d_{ij}^* \triangleq |\delta_{B,i}^{\text{char}} \delta_{A,j}^{\text{char}} - \delta_{A,i}^{\text{char}} \delta_{B,j}^{\text{char}}| \quad (36)$$

- The *weighted distance* from  $\eta_j^o$  to  $\eta_i^o$

$$d_{j \rightarrow i} \triangleq |\eta_i^o \delta_{A,j}^{\text{char}} + \delta_{B,j}^{\text{char}}| = \left| -\frac{\delta_{B,i}^{\text{char}}}{\delta_{A,i}^{\text{char}}} \delta_{A,j}^{\text{char}} + \delta_{B,j}^{\text{char}} \right| \quad (37)$$

From the definitions above, we have the following remarks:

- The weighted distance is a distance induced by  $(\delta_{A,j}^{\text{char}}, \delta_{B,j}^{\text{char}})$  at  $\eta_i^o$ , i.e.,  $l_{(\delta_{A,j}^{\text{char}}, \delta_{B,j}^{\text{char}})}(\eta_i^o) = |\eta_i^o \delta_{A,j}^{\text{char}} + \delta_{B,j}^{\text{char}}|$ . Note that  $d_{j \rightarrow i} \neq d_{i \rightarrow j}$  if  $|\delta_{A,i}^{\text{char}}| \neq |\delta_{A,j}^{\text{char}}|$ . That is, the distance induced by  $(\delta_{A,j}^{\text{char}}, \delta_{B,j}^{\text{char}})$  at  $\eta_i^o$  is not the same as the distance induced by  $(\delta_{A,j}^{\text{char}}, \delta_{B,j}^{\text{char}})$  at  $\eta_j^o$  in general.

- The relationships among Euclidean distance, normalized distance, and weighted distance are

$$d_{j \rightarrow i} = |\delta_{A,j}^{char}| d_{ij} = \frac{d_{ij}^*}{\delta_{A,i}^{char}} \quad (38)$$

- In Lemmas 2 and 3 below, we give a necessary condition and a sufficient condition for the distance-validity of  $(\delta_A, \delta_B)$ . In Lemma 6 below, we identify the minimum normalized distance associated with any zero- $l_{\min}$  channel gain using Lemmas 2 to 5.

*Symmetry of  $\mathbb{Z}[i]/q$  Under Rotations and Reflections:* In the following (including the Appendices), we assume w.l.o.g that  $q^R > q^I \geq 1$  when the proofs are given under a complex Gaussian prime  $q = q^R + iq^I$ ,  $|q| \geq \sqrt{5}$ , and  $q^R, q^I \neq 0$ . Due to the symmetry property of Gaussian primes, there is no loss of generality in assuming positive  $q^R$  and  $q^I$  within  $0 < \theta < \pi/4$  in the complex plane. Specifically, for a Gaussian prime  $q$ , rotations by multiples of  $\pi/2$  and reflections on the real and imaginary axes give other symmetric Gaussian primes. Similar symmetry applies to elements in  $\mathbb{Z}[i]$ . Therefore, elements in  $\mathbb{Z}[i]/q$  also undergo similar symmetric transformations.

*Lemma 2 (Necessary condition of validity):* Given a Gaussian prime  $q$  and  $q^R \neq 0, q^I \neq 0$ , if  $(\delta_A, \delta_B) \in \mathbb{Z}^2[i]$  is a distance-valid difference pair, then  $|\delta_A|, |\delta_B| \leq \sqrt{2|q|^2 - 4q^R + 2}$ .

The proof of Lemma 2 is given in Appendix II.

*Lemma 3 (Sufficient condition of validity):* Given a pair of Gaussian integers  $(\delta_A, \delta_B) \in \mathbb{Z}^2[i]$ , and a Gaussian prime  $q$  that defines valid symbols in  $\mathbb{Z}[i]$  according to Definition 1, a sufficient condition for  $(\delta_A, \delta_B)$  to be a distance-valid difference pair is  $|\delta_A| \neq 0$  or  $|\delta_B| \neq 0$  and  $|\delta_A|, |\delta_B| < |q|$ .

The proof of Lemma 3 is given in Appendix III.

Lemma 4 below is the well-known Bézout Identity in  $\mathbb{Z}[i]$  [21], [22].

*Lemma 4: [Bézout Identity in  $\mathbb{Z}[i]$ ]* Consider two Gaussian integers  $a$  and  $b$ , not both zero. There exist two Gaussian integers  $x$  and  $y$  such that  $ax - by = \gcd(a, b)$ . Furthermore, among the Gaussian integers that can be written in the form of  $ax' - by'$  where  $x'$  and  $y'$  are Gaussian integers, the  $x$  and  $y$  that satisfy  $ax - by = \gcd(a, b)$  yield the smallest possible norm for  $ax' - by'$  (i.e.,  $|\gcd(a, b)|^2$  is the smallest possible norm for  $ax' - by'$ ).

*Lemma 5:* Given a Gaussian prime  $q$ , for a distance-valid difference pair  $(\delta_{A,i}, \delta_{B,i})$  where  $\delta_{A,i} \in \{\pm 1, \pm i\}$  or  $\delta_{B,i} \in \{\pm 1, \pm i\}$ , there exists a distance-valid difference pair  $(\delta_{A,j}, \delta_{B,j})$  such that  $\delta_{A,j}\delta_{B,i} - \delta_{B,j}\delta_{A,i} = 1$ .

*Proof of Lemma 5:* W.l.o.g., consider  $\delta_{B,i} \in \{\pm 1, \pm i\}$ . For  $\delta_{A,j}\delta_{B,i} - \delta_{B,j}\delta_{A,i} = 1$ , we choose a distance-valid  $(\delta_{A,j}, \delta_{B,j}) = (\delta_{B,i}, 0)$  if  $\delta_{B,i} \in \{1, -1\}$  and  $(\delta_{A,j}, \delta_{B,j}) = (\delta_{B,i}^*, 0)$  if  $\delta_{B,i} \in \{i, -i\}$ , where  $*$  denotes complex conjugate.

Lemma 5 is similar to Bézout Identity for  $\mathbb{Z}[i]$  in Lemma 4 except that  $a$  and  $b$  are units, the RHS is a unit (i.e.,  $\gcd(a, b) = \{\pm 1, \pm i\}$ ), and that  $x$  and  $y$  are restricted to be components in a distance-valid difference pair  $(\delta_A, \delta_B)$ .

*Lemma 6:* Given a Gaussian prime  $q$ , for a nontrivial zero- $l_{\min}$  channel gain  $\eta_i^o$  associated with a characteristic difference  $(\delta_{A,i}^{char}, \delta_{B,i}^{char})$ , there exists a characteristic difference  $(\delta_{A,j}^{char}, \delta_{B,j}^{char})$  yielding  $|\delta_{A,j}^{char}\delta_{B,i}^{char} - \delta_{B,j}^{char}\delta_{A,i}^{char}| = 1$

*Proof of Lemma 6:*

For  $|q| = \sqrt{2}$ , the validity of the lemma can be easily verified. Specifically, for  $|q| = \sqrt{2}$ , the representative elements in  $\mathbb{Z}[i]/q$  are limited to the two values in the set  $\{0, 1\}$ . The nontrivial zero- $l_{\min}$  channel gains can only be  $\eta_i^o = -\delta_{B,i}^{char}/\delta_{A,i}^{char} = 1$  or  $-1$ . To satisfy  $|\delta_{A,j}^{char}\delta_{B,i}^{char} - \delta_{B,j}^{char}\delta_{A,i}^{char}| = 1$ , we can simply let  $\delta_{A,j}^{char} = \delta_{B,i}^{char}$  and  $\delta_{B,j}^{char} = 0$ .

We now consider  $|q| \geq \sqrt{5}$ . The proof consists of two parts P1) and P2). In P1), we prove that given a Gaussian prime  $q$ , there exists a distance-valid difference pair  $(\delta_{A,j}, \delta_{B,j})$  such that

$$\delta_{A,j}\delta_{B,i}^{char} - \delta_{B,j}\delta_{A,i}^{char} = 1. \quad (39)$$

In P2), we prove that  $\gcd(\delta_{A,j}, \delta_{B,j}) = 1$ , i.e.,  $(\delta_{A,j}, \delta_{B,j})$  is a characteristic difference.

**P1)** Given a Gaussian prime  $q$ , the case where  $\delta_{A,i} \in \{\pm 1, \pm i\}$  or  $\delta_{B,i} \in \{\pm 1, \pm i\}$  has been covered by Lemma 5. Our proof here focuses on the case where  $\delta_{A,i} \notin \{\pm 1, \pm i\}$  and  $\delta_{B,i} \notin \{\pm 1, \pm i\}$ .

By Lemma 4, given a Gaussian prime  $q$ , there exist Gaussian integers  $x$  and  $y$  such that

$$x\delta_{B,i}^{char} - y\delta_{A,i}^{char} = 1. \quad (40)$$

Now,  $(x, y)$  may or may not be a distance-valid difference pair. However, given that  $(x, y)$  is a solution to (40), the following are also solutions:

$$\begin{aligned} \delta_{A,j} &= x + k\delta_{A,i}^{char} \\ \delta_{B,j} &= y + k\delta_{B,i}^{char}, \end{aligned} \quad (41)$$

for all Gaussian integers  $k$ . Our goal is to show that there exists a  $k \in \mathbb{Z}[i]$  such that  $(\delta_{A,j}, \delta_{B,j})$  is distance-valid.

This paragraph shows that there exist  $\delta_{A,j}$  for some  $k \in \mathbb{Z}[i]$  in (41) such that  $0 < |\delta_{A,j}| < |q|$ . By [21, Theorem 3.1], for  $\delta_{A,i}^{char}$  where  $|\delta_{A,i}^{char}|^2 > 1$  (i.e.,  $\delta_{A,i}^{char} \notin \{\pm 1, \pm i\}$ ), there exists a  $k \in \mathbb{Z}[i]$  such that

$$|\delta_{A,j}|^2 \leq \frac{1}{2}|\delta_{A,i}^{char}|^2 \quad (42)$$

Thus,  $|\delta_{A,j}|^2 \leq \frac{1}{2}|\delta_{A,i}^{char}|^2 \leq \frac{1}{2}(2|q|^2 - 4q^R + 2) < |q|^2$ , where the second inequality is due to the necessary condition in Lemma 2. Furthermore,  $\delta_{A,j} \neq 0$  (otherwise, we would have  $\delta_{B,j}\delta_{A,i}^{char} = -1$  in (39), implying  $|\delta_{A,i}^{char}|^2 = 1$ ; but the proof here assumes  $|\delta_{A,i}^{char}|^2 > 1$  since the case  $|\delta_{A,i}^{char}|^2 = 1$  has been covered by Lemma 5).

The next few paragraphs show that given the  $\delta_{A,j}$  found in the previous paragraph, the corresponding  $\delta_{B,j}$  that satisfies (41) is such that  $0 < |\delta_{B,j}| < |q|$ . Thus, the pair  $(\delta_{A,j}, \delta_{B,j})$  is distance-valid according to Lemma 3. Recall that the pair  $(\delta_{A,j}, \delta_{B,j})$  must satisfy (39). With respect to (39), Fig. 7 below draws the relationship between the vectors  $\delta_{A,j}\delta_{B,i}^{char}$ ,  $-\delta_{B,j}\delta_{A,i}^{char}$  and 1 in the complex plane:



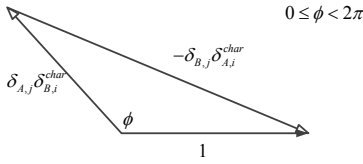


Fig. 7. The triangle formed by the vectors  $\delta_{A,j}\delta_{B,i}^{char}$ ,  $-\delta_{B,j}\delta_{A,i}^{char}$ , and 1.

By cosine rule,

$$\begin{aligned} |\delta_{B,j}\delta_{A,i}^{char}|^2 &= |\delta_{A,j}\delta_{B,i}^{char}|^2 + 1 - 2|\delta_{A,j}\delta_{B,i}^{char}|\cos\phi \\ &\leq |\delta_{A,j}\delta_{B,i}^{char}|^2 + 1 + 2|\delta_{A,j}\delta_{B,i}^{char}|. \end{aligned} \quad (43)$$

Then, we have

$$\begin{aligned} |\delta_{B,j}|^2 &\leq \frac{|\delta_{A,j}\delta_{B,i}^{char}|^2 + 1 + 2|\delta_{A,j}\delta_{B,i}^{char}|}{|\delta_{A,i}^{char}|^2} \\ &\leq \frac{1}{2}|\delta_{B,i}^{char}|^2 + \frac{1}{2} + \sqrt{2}\frac{|\delta_{B,i}^{char}|}{|\delta_{A,i}^{char}|}, \end{aligned} \quad (44)$$

where the second inequality is due to (42) and  $|\delta_{A,i}^{char}|^2 > 1$ , because the case where  $|\delta_{A,i}^{char}| = 1$  has been covered by Lemma 5.

W.l.o.g., we assume  $\frac{|\delta_{B,i}^{char}|}{|\delta_{A,i}^{char}|} \leq 1$  (alternatively, if  $\frac{|\delta_{B,i}^{char}|}{|\delta_{A,i}^{char}|} > 1$ , we switch the roles of A and B in (42) and a similar argument follows after that).

Given  $|q| \geq \sqrt{5}$  there are two possibilities:  $q$  is real or  $q$  is complex. For real  $q$ , we have  $q^R = |q| \geq 2$ . For complex  $q$ , w.l.o.g., we assume  $q^R > q^I \geq 1$ . (note: for a given complex  $q$  with  $|q| \geq \sqrt{5}$ , we can always find one  $q$  such that  $q^R > q^I \geq 1$ ; the proofs are similar for other cases if we apply the symmetry of  $\mathbb{Z}[i]$  and  $\mathbb{Z}[i]/q$  to our previous lemmas and the proof here). Thus, overall, whether  $q$  is real or complex, we have  $q^R \geq 2$ . Continuing from (44), we have

$$\begin{aligned} |\delta_{B,j}|^2 &\leq \frac{1}{2}|\delta_{B,i}^{char}|^2 + \frac{1}{2} + \sqrt{2} \\ &\leq \frac{1}{2}(2|q|^2 - 6) + \frac{1}{2} + \sqrt{2} < |q|^2, \end{aligned} \quad (45)$$

where the second inequality holds since  $|\delta_{B,i}^{char}|^2 \leq 2|q|^2 - 6$  by substituting  $q^R \geq 2$  in  $\sqrt{2|q|^2 - 4q^R} + 2$  in the statement of Lemma 2.

Furthermore,  $\delta_{B,j} \neq 0$  since if  $\delta_{B,j} = 0$ , (39) would become  $\delta_{A,j}\delta_{B,i}^{char} = 1$ , but we are not considering the case where  $|\delta_{B,i}^{char}|^2 = 1$  here since it has been covered by Lemma 5.

**P2)** Suppose that the distance-valid  $(\delta_{A,j}, \delta_{B,j})$  found in P1) are not coprime in  $\mathbb{Z}[i]$ , i.e.,  $\gcd(\delta_{A,j}, \delta_{B,j}) = d$  and  $|d|^2 > 1$ . By Lemma 3, there exist some  $(x', y') \in \mathbb{Z}[i]$  such that  $x'\delta_{A,j} + y'\delta_{B,j} = d$ , and  $|d|^2$  is the smallest norm of  $x'\delta_{A,j} + y'\delta_{B,j}$ . However, the smallest norm of  $x'\delta_{A,j} + y'\delta_{B,j}$  is 1 from (39), contradicting  $|d|^2 > 1$ . ■

## VI. WEIGHTED VORONOI REGION OF ZERO- $l_{\min}$ CHANNEL GAINS

Section V analyzed the distance properties at zero- $l_{\min}$  channel gains. This section moves on to the study of general channel gains where  $l_{\min}$  is not necessary zero. Intuitively,

for channel gains  $\eta$  in the near neighborhood of a zero- $l_{\min}$  channel gain  $\eta_i^o$ , the linear NC mapping  $(\alpha_{opt}, \beta_{opt}) = (-(\delta_{A,i}^{char(q)})^{-1}\delta_{B,i}^{char(q)}, 1)$  for  $\eta_i^o$  is still optimal in that it will still yield the largest possible  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ . In general, as we will see, the complex plane of  $\eta$  can be partitioned into multiple Voronoi regions, with each region containing exactly one at zero- $l_{\min}$  channel gain and that the optimal NC mapping  $(\alpha_{opt}, \beta_{opt})$  for that  $\eta^o$  applies to all  $\eta$  within the Voronoi region of  $\eta^o$ .<sup>1</sup>

With reference to Fig. 5, the set of channel gains that should adopt the NC mapping  $(\alpha_{opt}, \beta_{opt}) = (-(\delta_{A,i}^{char(q)})^{-1}\delta_{B,i}^{char(q)}, 1)$  is given by

$$\begin{aligned} \mathcal{V}(\eta_i^o) &\triangleq \{\eta \in \mathbb{C} \mid d_{\eta_i^o \rightarrow \eta} \leq d_{\eta_j^o \rightarrow \eta}, \forall j \neq i\} \\ &= \{\eta \in \mathbb{C} \mid |\delta_{A,i}^{char}\eta + \delta_{B,i}^{char}| \leq |\delta_{A,j}^{char}\eta + \delta_{B,j}^{char}|, \forall j \neq i\}. \end{aligned} \quad (46)$$

In other words, for an  $\eta \in \mathcal{V}(\eta_i^o)$ ,  $l_{\min}(\eta)$  is given by  $|\delta_{A,i}^{char}\eta + \delta_{B,i}^{char}|$  and not by  $|\delta_{A,j}^{char}\eta + \delta_{B,j}^{char}|$ ,  $j \neq i$ . Note that in (46), we have generalized the definition of the weighted distance from one zero- $l_{\min}$  channel gain to another zero- $l_{\min}$  channel gain in (37) to a weighted distance from a zero- $l_{\min}$  channel gain  $\eta_i^o$  to a general channel gain  $\eta$  to as follows:

$$d_{\eta_i^o \rightarrow \eta} = |\delta_{A,i}^{char}\eta + \delta_{B,i}^{char}|. \quad (47)$$

We refer to  $\mathcal{V}(\eta_i^o)$  as the weighted Voronoi region of  $\eta_i^o$ .

Section V showed that for  $\eta = \eta_i^o$ ,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})} = \frac{1}{|\delta_{A,i}^{char}|}$  and that there is always another characteristic difference  $(\delta_{A,j}^{char}, \delta_{B,j}^{char})$  whose normalized distance with respect to  $(\delta_{A,i}^{char}, \delta_{B,i}^{char})$  is one—i.e.,  $|\delta_{A,j}\delta_{B,i} - \delta_{B,j}\delta_{A,i}| = 1$ . For a general  $\eta$  within the Voronoi region of  $\eta_i^o$ , however, the situation is more complicated. In general,  $\eta_i^o$  may have several neighbors whose Voronoi regions share a boundary with  $\eta_i^o$  and the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  at a particular  $\eta \in \mathcal{V}(\eta_i^o)$  is the weighted distance of one of these neighbors to  $\eta$ ; however,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  at different  $\eta \in \mathcal{V}(\eta_i^o)$  may be determined by the weighted distances of different neighbors. The normalized distance between some of these neighbors and  $(\delta_{A,j}^{char}, \delta_{B,j}^{char})$  may be larger than one.

### A. Preliminaries on the Weighted Voronoi Region

Fig. 8 shows the weighted Voronoi region of  $\eta_0^o$  in the complex plane of  $\eta$ . Illustrated by this figure, we introduce some definitions and essential properties of the weighted Voronoi region [25]–[27].

In the complex plane of  $\eta$ , we consider a set of distinct generators  $\{\eta_0^o, \eta_1^o, \dots, \eta_I^o\}$  (generators are simply zero- $l_{\min}$  channel gains in our problem) and assign a weight  $\delta_i$  to each  $\eta_i^o$ . With this weight, we define a distance from the generator  $\eta_i^o$  to any other point as a weighted distance  $d_{\eta_i^o \rightarrow \eta}$  from  $\eta_i^o$  to  $\eta$ :

$$d_{\eta_i^o \rightarrow \eta} \triangleq |\delta_i(\eta_i^o - \eta)|. \quad (48)$$

<sup>1</sup>As far as  $l_{\min}$  analysis is concerned, the Voronoi-region analysis in this section applies to both linear and nonlinear PNC mappings; it is the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  analysis in Part F that applies specifically to linear PNC mapping. In particular, our  $l_{\min}$  analysis for complex modulations also applies to nonlinear PNC, should someone wants to further study nonlinear PNC.



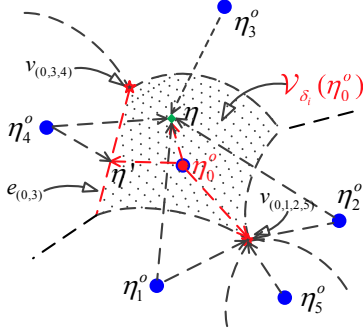


Fig. 8. The weighted Voronoi of  $\eta_0^o$  and its adjacent regions.

**Weighted Voronoi Region:** The weighted Voronoi region of  $\eta_i^o$  is defined as (see the shaded region in Fig. 8)

$$\mathcal{V}(\eta_i^o) \triangleq \{\eta \in \mathbb{C} | d_{\eta_i^o \rightarrow \eta} \leq d_{\eta_j^o \rightarrow \eta}, \forall j \neq i\}. \quad (49)$$

Given any point  $\eta \in \mathcal{V}(\eta_i^o)$ , the weighted distance from  $\eta_i^o$  to  $\eta$  is no more than that from  $\eta_j^o$  to  $\eta$ ,  $\forall j \neq i$ . We call  $\eta_i^o$  of  $\mathcal{V}(\eta_i^o)$  the *generator* of the weighted Voronoi region.

**Voronoi Edge:** A closed weighted Voronoi region of  $\eta_i^o$  contains its boundary that consists of straight lines and circular arcs, which we call weighted Voronoi edges. Mathematically, if  $\mathcal{V}(\eta_i^o) \cap \mathcal{V}(\eta_j^o) \neq \emptyset$ , the set  $\mathcal{V}(\eta_i^o) \cap \mathcal{V}(\eta_j^o)$  gives a Voronoi edge (which may degenerate into a point). We denote a Voronoi edge shared by  $\mathcal{V}(\eta_i^o)$  and  $\mathcal{V}(\eta_j^o)$  as

$$e_{(i,j)} \triangleq \{\eta \in \mathbb{C} | d_{\eta_i^o \rightarrow \eta} = d_{\eta_j^o \rightarrow \eta}, \forall j \neq i\}. \quad (50)$$

That is, given any  $\eta$  on the edge  $e_{(i,j)}$ , the weighted distance from  $\eta_i^o$  to  $\eta$  is the same as the weighted distance from  $\eta_j^o$  to  $\eta$ . In particular, in the complex plane with the coordinates  $(\eta^R, \eta^I)$ , an edge is a circular arc if and only if the weights of the weighted Voronoi regions sharing the edge are different, i.e.,

$$\begin{aligned} e_{(i,j)} : |\delta_{A,i}^{char}(\eta_i^o - \eta)| &= |\delta_{A,j}^{char}(\eta_j^o - \eta)| \Rightarrow \\ & \left( \eta^R - \frac{(\eta_i^o)^R |\delta_{A,i}^{char}|^2 - (\eta_j^o)^R |\delta_{A,j}^{char}|^2}{|\delta_{A,i}^{char}|^2 - |\delta_{A,j}^{char}|^2} \right)^2 \\ & + \left( \eta^I - \frac{(\eta_i^o)^I |\delta_{A,i}^{char}|^2 - (\eta_j^o)^I |\delta_{A,j}^{char}|^2}{|\delta_{A,i}^{char}|^2 - |\delta_{A,j}^{char}|^2} \right)^2 \\ & = \frac{|\delta_{A,i}^{char}|^2 |\delta_{A,j}^{char}|^2}{(|\delta_{A,i}^{char}|^2 - |\delta_{A,j}^{char}|^2)^2} [((\eta_i^o)^R - (\eta_j^o)^R)^2 + ((\eta_i^o)^I - (\eta_j^o)^I)^2], \end{aligned}$$

and an edge is a straight line if and only if the weights of the weighted Voronoi regions sharing the edge are the same, i.e.,

$$\begin{aligned} e_{(i,j)} : |\eta_i^o - \eta| &= |\eta_j^o - \eta| \Rightarrow \\ \eta^I &= \frac{(\eta_i^o)^R - (\eta_j^o)^R}{(\eta_j^o)^I - (\eta_i^o)^I} \eta^R + \frac{|\eta_j^o|^2 - |\eta_i^o|^2}{2(\eta_j^o)^I - (\eta_i^o)^I}. \quad (51) \end{aligned}$$

Note that  $e_{(i,j)}$  is empty if  $\mathcal{V}(\eta_i^o) \cap \mathcal{V}(\eta_j^o) = \emptyset$ . In Fig. 8, the red dashed line  $e_{(0,3)}$  is a Voronoi edge shared by  $\mathcal{V}(\eta_0^o)$  and  $\mathcal{V}(\eta_3^o)$ .

**Voronoi Vertex:** An end point of a Voronoi edge is called a Voronoi vertex. We denote a Voronoi vertex shared by three or more Voronoi regions  $\mathcal{V}(\eta_i^o), \mathcal{V}(\eta_j^o), \mathcal{V}(\eta_k^o), \dots$  as

$$\begin{aligned} e_{(i,j,k,\dots)} &\triangleq \{\eta \in \mathbb{C} | d_{\eta_i^o \rightarrow \eta} = d_{\eta_j^o \rightarrow \eta} = d_{\eta_k^o \rightarrow \eta} = \dots, \\ & \quad \forall j \neq k \neq i \neq \dots\}. \quad (52) \end{aligned}$$

In Fig. 8,  $\mathcal{V}(\eta_0^o)$ ,  $\mathcal{V}(\eta_3^o)$ , and  $\mathcal{V}(\eta_4^o)$  meet at a Voronoi vertex  $v_{(0,3,4)}$ .

**Adjacent Voronoi Regions:** Two Voronoi regions are said to be adjacent if the Voronoi regions share a Voronoi edge or a Voronoi vertex. We also say that two characteristic differences,  $(\delta_{A,i}^{char}, \delta_{B,i}^{char})$  and  $(\delta_{A,j}^{char}, \delta_{B,j}^{char})$ , are adjacent if their associated Voronoi regions,  $\mathcal{V}(-\frac{\delta_{B,i}^{char}}{\delta_{A,i}^{char}})$  and  $\mathcal{V}(-\frac{\delta_{B,j}^{char}}{\delta_{A,j}^{char}})$ , are adjacent.

In Fig. 8,  $\mathcal{V}(\eta_0^o)$  and  $\mathcal{V}(\eta_4^o)$  are adjacent since they share the same edge  $e_{(0,4)}$ , and  $\mathcal{V}(\eta_0^o)$ ,  $\mathcal{V}(\eta_1^o)$ ,  $\mathcal{V}(\eta_2^o)$ , and  $\mathcal{V}(\eta_3^o)$  are adjacent since they meet at a point  $v_{(0,1,2,5)}$ .

### B. Optimal NC mapping of Voronoi Regions

In this part, we show that the optimal NC mapping for an arbitrary  $\eta \in \mathcal{V}(\eta_0^o)$  is  $(-\delta_A^{char(q)} - 1 \delta_B^{char(q)}, 1)$ , the same as that for  $\eta = \eta^o$ , when  $\eta^o$  is a nontrivial zero- $l_{\min}$  channel gain.

**Remark 7:** For the two trivial zero- $l_{\min}$  channel gains  $\eta^o = 0$  and  $\eta^o = \infty$ , we cannot find an NC mapping to cluster  $(\delta_A^{char}, \delta_B^{char}) = (1, 0)$  which induces a zero  $l_{\min}$  at  $\eta^o = 0$ , and to cluster  $(\delta_A^{char}, \delta_B^{char}) = (1, 0)$  which induces a zero  $l_{\min}$  at  $\eta^o = \infty$ . Both  $(\delta_A^{char}, \delta_B^{char}) = (1, 0)$  and  $(\delta_A^{char}, \delta_B^{char}) = (0, 1)$  are distance-valid, but not NC-valid, characteristic differences. See *Trivial Theorem* in Section V for details. Extrapolating this observation to the Voronoi region of  $\eta^o = 0$  and  $\eta^o = \infty$ , we conclude that  $d_{\min}(\eta) = l_{\min}(\eta)$  within their Voronoi regions. ■

**Theorem 3:** Consider a nontrivial zero- $l_{\min}$  channel gain  $\eta^o$  associated with the characteristic difference  $(\delta_A^{char}, \delta_B^{char})$ . For all  $\eta \in \mathcal{V}(\eta^o)$ , the optimal NC mapping is the same as that for the zero- $l_{\min}$  channel gain  $\eta^o$ , i.e.,  $(\alpha_{opt}, \beta_{opt}) = (-\delta_A^{char(q)} - 1 \delta_B^{char(q)}, 1)$ .

**Proof of Theorem 3:**  $l_{\min}$  at an arbitrary  $\eta \in \mathcal{V}(\eta^o)$  is the weighted distance from the generator  $\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$  to  $\eta$ , i.e.,  $l_{\min}(\eta) = l_{(\delta_A^{char}, \delta_B^{char})}(\eta) = |\eta \delta_A^{char} + \delta_B^{char}|$  for  $\eta \in \mathcal{V}(\eta^o)$ . If  $\eta = \eta^o$ , then the optimal NC mapping follows from *Theorem 2* for the zero- $l_{\min}$  channel gain. If  $\eta \neq \eta^o$  and  $\eta \in \mathcal{V}(\eta^o)$ , we have  $l_{\min} > 0$ . In this case, to ensure  $d_{\min}^{(\alpha_{opt}, \beta_{opt})} \geq l_{\min} > 0$ , we need to cluster  $(\delta_A^{char}, \delta_B^{char})$ . Otherwise,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})} = l_{\min}$ . Similar to the proof of *Theorem 2*, the solution for this clustering is  $(\alpha_{opt}, \beta_{opt}) = (-\delta_A^{char(q)} - 1 \delta_B^{char(q)}, 1)$ . Once  $(\delta_A^{char}, \delta_B^{char})$  is clustered, the NC partitioning is fixed, and there is no further freedom to cluster another NC-valid difference pair that does not belong to the clustered-difference set of  $(\alpha_{opt}, \beta_{opt})$ . ■

### C. Identifying $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ in Voronoi Regions

In Section V, we have identified  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  at zero- $l_{\min}$  channel gains. This part aims to identify  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  for general channel gains. Let us consider  $\eta$  in a particular Voronoi region generated by zero- $l_{\min}$  channel gain  $\eta^o$ . To explicitly identify the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference, we first consider an exhaustively search method as follows, before putting forth an efficient method for doing so in *Theorem 4*.

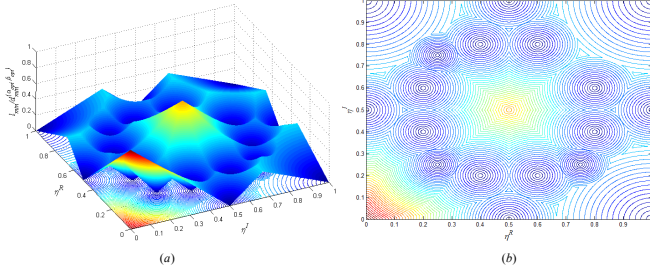


Fig. 9. (a)  $l_{\min}(\eta)$  for  $\eta \notin \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$  and  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}(\eta)$  versus  $\eta \in \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$ , where  $(\delta_A^{\text{char}}, \delta_B^{\text{char}}) = (1 + i, -i)$  and  $q = 3$ ; (b) the corresponding contour graphs of  $l_{\min}(\eta)$  and  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}(\eta)$ .

As shown in Fig. 9, one way to find the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining difference at an  $\eta \in \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$  is to first remove the characteristic difference  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  and the other clustered differences of  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  (i.e., remove difference pairs in the clustered-difference set  $\Delta_{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ ), and then numerically search for the new characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that determines the “new”  $l_{\min}$  for  $\eta \in \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$  in the absence of difference pairs in  $\Delta_{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ . The  $l_{\min}$  for an  $\eta \in \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$  in the absence of  $\Delta_{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  is the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  at this  $\eta$ , and  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  is the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining difference at this  $\eta$ .

We formally define and describe “removal of the characteristics differences” as follows (an illustrating example is given in Fig. 9):

**Removal of Characteristic Differences Induced by Optimal NC mapping (ROCD):** The optimal NC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  removes the difference pairs in  $\Delta_{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  from consideration in the process of finding the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining differences at an arbitrary  $\eta \in \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$ . Specifically, after the removal of such difference pairs, we redraw the Voronoi regions of the remaining characteristic differences. The other characteristic differences “close to”  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  may divide the region among them so that their “new” Voronoi regions may include part of the old  $\mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$ . The “new”  $l_{\min}$  associated with an  $\eta \in \mathcal{V}(-\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}})$  is the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  for that  $\eta$ .

Theorem 4 below puts forth an efficient approach to identify the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining differences at an arbitrary  $\eta \in \mathcal{V}(\eta^o)$  by stating that only characteristic differences adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  can be  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining differences.

**Theorem 4:** Consider an arbitrary channel gain  $\eta \in \mathcal{V}(\eta^o)$ , where  $\eta^o = -\frac{\delta_B^{\text{char}}}{\delta_A^{\text{char}}}$  is a nontrivial zero- $l_{\min}$  channel gain associated with the characteristic difference  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ . With the optimal NC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$ , the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$ -determining difference at this  $\eta$  is a characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that is adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ .

*Proof of Theorem 4:*

Our proof depends on two results that will be proved later in Part F:

- (T4-1)  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  cannot cluster any characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that is adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ .
- (T4-2) For any characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  that is not adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ , given any  $\eta \in \mathcal{V}(\eta^o)$ , there exists a characteristic difference  $(\delta_A^{\text{char}'}, \delta_B^{\text{char}'})$  adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  such that  $|\eta \delta_B^{\text{char}''} + \delta_A^{\text{char}''}| > |\eta \delta_B^{\text{char}'} + \delta_A^{\text{char}'}| \forall \eta \in \mathcal{V}(\eta^o) \setminus \{\eta^o\}$ , and  $|\eta \delta_B^{\text{char}''} + \delta_A^{\text{char}''}| \geq |\eta \delta_B^{\text{char}'} + \delta_A^{\text{char}'}|$  at  $\eta = \eta^o$ .

(T4-2) means that given any  $\eta \in \mathcal{V}(\eta^o)$  and a non-adjacent characteristic difference, there is always an adjacent characteristic difference that is closer to  $\eta$  than any given non-adjacent characteristic difference. (T3-1) says that this adjacent characteristic difference cannot be clustered by the optimal NC mapping  $(\alpha_{\text{opt}}, \beta_{\text{opt}})$  applied within  $\mathcal{V}(\eta^o)$ . Thus, under ROCD, the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  within  $\mathcal{V}(\eta^o)$  must be determined by characteristic differences adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ , and not by non-adjacent characteristic differences.

**Remark 8:** Note that for different  $\eta$  within  $\mathcal{V}(\eta^o)$ , the  $d_{\min}^{(\alpha_{\text{opt}}, \beta_{\text{opt}})}$  may be determined by different characteristic differences, but they must all be adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$ .

The proof of (T4-1) requires some background to be established regarding the properties of adjacent characteristic differences (specifically, the normalized distances between a characteristic difference and its adjacent characteristic differences). Parts D and E below will first establish this background. Part F will then provide the proofs for (T4-1) and (T4-2).

#### D. Notations and Definitions

In Part E, we will put forth an efficient way to identify characteristic differences that are adjacent to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  through their normalized distances to  $(\delta_A^{\text{char}}, \delta_B^{\text{char}})$  and other properties. We will draw heavily on the formalism in [23] when deriving our results. For easy cross-reference by the reader, we redefine some notations in this part for consistency with the notations used in [23]. In addition, we also put forth some new definitions in preparation for the discussion in Part E.

**Notation Modifications:** We express a zero- $l_{\min}$  channel gain  $\eta^o$  as a ratio of two Gaussian integers, e.g.,  $(\kappa, \tau)$ . Then, we have  $\eta^o = \frac{\kappa}{\tau}$  where  $\kappa = -\delta_B^{\text{char}}$  and  $\tau = \delta_A^{\text{char}}$  (note: we have switched the position of  $(\delta_A, \delta_B)$  in  $(\kappa, \tau)$  since this is notation used in [23]). Thus,  $\gcd(\kappa, \tau) = 1$ . Furthermore, we denote the weighted Voronoi region of  $(\kappa, \tau)$  as  $\mathcal{V}(\frac{\kappa}{\tau})$ .

With respect to (8), we have defined  $\Delta$  as the set of distance-valid difference pairs induced by elements of  $\mathbb{Z}[i]/q$  for some Gaussian primes  $q$ . Here, we define the subset of  $\Delta$  that collects all characteristic differences in  $\Delta$  as the  $\mathcal{Q}_q^{\text{char}}$ -set:

$$\mathcal{Q}_q^{\text{char}} \triangleq \{(\kappa, \tau) | (-\tau, \kappa) \in \Delta, \gcd(\kappa, \tau) = 1\}. \quad (53)$$

Note that by definition of  $\Delta$ ,  $\kappa$  and  $\tau$  cannot both be zero at the same time.

With respect to (53), the elements in  $\mathcal{Q}_q^{\text{char}}$ -set form a generalized *Farey Sequence* in  $\mathbb{Z}[i]$  [23]. Each element in the Farey Sequence is an irreducible fraction  $\frac{\kappa}{\tau}$ ,  $(\kappa, \tau) \in \Delta$ . There

is a bijective mapping between the elements in the  $\mathcal{Q}_q^{char}$ -set and the elements in the associated Farey Sequence.

We further define a dual set of  $\mathcal{Q}_q^{char}$ -set as follows:

$$\mathcal{Q}_q \triangleq \{(\kappa, \tau) \in \mathbb{Z}^2[i] \mid \exists v \in \{\pm 1, \pm i\}, (\frac{v\kappa}{\gcd(\kappa, \tau)}, \frac{v\tau}{\gcd(\kappa, \tau)}) \in \mathcal{Q}_q^{char}\}. \quad (54)$$

Let us elaborate the definition in (54). First, let us write  $(\kappa', \tau') = (\frac{v\kappa}{\gcd(\kappa, \tau)}, \frac{v\tau}{\gcd(\kappa, \tau)})$ . Obviously,  $\frac{\kappa'}{\tau'}$  is an *irreducible* fraction. According to the above definition, if  $(\kappa', \tau') \in \mathcal{Q}_q^{char}$ , then  $(\kappa, \tau) \in \mathcal{Q}_q$ . Furthermore, we note that gcd of two Gaussian integers is not unique. If  $x$  is a particular gcd of  $\kappa$  and  $\tau$ , so are  $-x, ix, -ix$ . In general, there are four possible ways to reduce  $(\kappa, \tau)$  to  $(\kappa', \tau')$ . In (54), we write  $(\kappa', \tau') = (\frac{v\kappa}{\gcd(\kappa, \tau)}, \frac{v\tau}{\gcd(\kappa, \tau)})$ , where  $\gcd(\kappa, \tau)$  refers specifically to one of the four possible gcd's. Now, in general, it is possible for some of the  $(\kappa', \tau')$  to belong to the set  $\mathcal{Q}_q^{char}$  and some not. According to our definition in (54), we require only at least one of the four  $(\kappa', \tau')$  to belong to the set  $\mathcal{Q}_q^{char}$  in order that  $(\kappa, \tau) \in \mathcal{Q}_q$ . That is,  $(\kappa, \tau) \in \mathcal{Q}_q$  if there is a  $v \in \{\pm 1, \pm i\}$  such that  $(\kappa', \tau') \in \mathcal{Q}_q^{char}$ .

Two elements  $(\kappa', \tau') \in \mathcal{Q}_q^{char}$  and  $(\kappa, \tau) \in \mathcal{Q}_q$  are said to be *equivalent* if  $\frac{\kappa'}{\tau'} = \frac{\kappa}{\tau}$ . These two ratios are the same and they correspond to the same zero- $l_{\min}$  channel gain in the communication problem of this paper. The reason for defining  $\mathcal{Q}_q$  is for the convenience of the statements of some lemmas and proofs later (specifically, *Q-criteria 1-3*). In the proofs, when we identify a pair  $(\kappa, \tau) \in \mathcal{Q}_q$ , that means we have also identified a pair  $(\kappa', \tau') \in \mathcal{Q}_q^{char}$ .

Now, our problem can be reformulated as how to characterize the weighted Voronoi regions of elements in  $\mathcal{Q}_q^{char}$ -set. Clearly, the weighted Voronoi region of each element in  $\mathcal{Q}_q^{char}$ -set is bounded by a finite set of lines and arcs, and these boundaries are generated by the adjacent Voronoi regions. From the definition of adjacent Voronoi regions, two pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$  are said to be adjacent if the weighted Voronoi regions  $\mathcal{V}(\frac{\kappa}{\tau})$  and  $\mathcal{V}(\frac{\gamma}{\delta})$  have a point  $z'$  in common (note:  $z'$  here is  $\eta$  in precious sections), i.e.,

$$d_{\frac{\kappa}{\tau} \rightarrow z'} = d_{\frac{\gamma}{\delta} \rightarrow z'} = |\tau(\frac{\kappa}{\tau} - z')| = |\delta(\frac{\gamma}{\delta} - z')| \\ = \min_{\forall(\zeta, \vartheta) \in \mathcal{Q}_q^{char}} |\vartheta(\frac{\zeta}{\vartheta} - z')| = \min_{\forall(\tilde{\zeta}, \tilde{\vartheta}) \in \mathcal{Q}_q} |\tilde{\vartheta}(\frac{\tilde{\zeta}}{\tilde{\vartheta}} - z')|. \quad (55)$$

Before we detail our approach to identify the adjacent regions, let us introduce some relevant results from [23] that provides useful insights to solve our problem. Specifically, [23] developed a systematic way to study the approximation of complex numbers by numbers of the quadratic field  $\mathbb{Q}(\sqrt{-1})$  (i.e., approximating complex numbers by Gaussian rationals formed by ratios of two Gaussian integers  $\mathbb{Z}[i]$ , in a way that is analogous to approximating real numbers by rational numbers). The approximation problem can also be characterized by identifying the weighted Voronoi regions of a set of generators drawn from  $\mathbb{Q}(\sqrt{-1})$ , i.e., all complex numbers in a Voronoi region is approximated by its generator. However, [23] considered a different set of irreducible fractions  $\frac{\kappa}{\tau}$  such that  $|\kappa|^2, |\tau|^2 \leq N$ , where  $N$  is a real integer. In this paper, we

define the set Gaussian integers used in [23] as the  $\mathcal{N}_N^{char}$ -set and the  $\mathcal{N}_N$ -set:<sup>2</sup>

$$\mathcal{N}_N^{char} \triangleq \{(\kappa, \tau) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\} \mid \gcd(\kappa, \tau) = 1, |\kappa|^2, |\tau|^2 \leq N\}, \quad (56)$$

$$\mathcal{N}_N \triangleq \{(\kappa, \tau) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\} \mid (\frac{\kappa}{\gcd(\kappa, \tau)}, \frac{\tau}{\gcd(\kappa, \tau)}) \in \mathcal{N}_N^{char}\}. \quad (57)$$

*Remark 9:* Note that both  $\mathcal{N}_N^{char}$  and  $\mathcal{N}_N$  have the symmetry property, i.e. given a  $(\kappa, \tau)$  in  $\mathcal{N}_N^{char}$  and  $\mathcal{N}_N$ , we can find the other three elements as  $\{-(\kappa, \tau), i(\kappa, \tau), -i(\kappa, \tau)\}$  symmetric to  $(\kappa, \tau)$  also in  $\mathcal{N}_N^{char}$  and  $\mathcal{N}_N$ , due to  $|\kappa|^2, |\tau|^2 \leq N$ . However, depending on  $q$ ,  $\mathcal{Q}_q^{char}$  and  $\mathcal{Q}_q$  may not retain this symmetry. To see this, we know that the elements in  $\mathcal{Q}_q^{char}$  and  $\mathcal{Q}_q$  are induced from any two distinct elements in  $\mathbb{Z}[i]/q$  with a Gaussian prime  $q$ . The elements in  $\mathbb{Z}[i]/q$  may not be symmetric, i.e., given  $(w_A, w_B) \in \mathbb{Z}[i]/q$ , we have  $v(w_A, w_B) \notin \mathbb{Z}[i]/q$  for some  $v \in \{\pm 1, \pm i\}$ . Therefore, we need to specify  $v$  that yields  $v(\frac{\kappa}{\gcd(\kappa, \tau)}, \frac{\tau}{\gcd(\kappa, \tau)}) \in \mathcal{Q}_q^{char}$  for  $(\kappa, \tau) \in \mathcal{Q}_q$  in (54). In (57), either all four ways of reducing  $(\kappa, \tau)$  give rise to an element in  $\mathcal{N}_N^{char}$ , or none of the four reductions does. Hence, we do not distinguish the four ways of reduction in the definition of  $\mathcal{N}_N$  in (57). ■

Given an arbitrary pair  $(\kappa, \tau) \in \mathcal{N}_N^{char}$ , [23] gives a selection criterion to find distinct elements in  $\mathcal{N}_N^{char}$ -set that are adjacent to  $(\kappa, \tau)$ . We refer to it as  $\mathcal{N}$ -criterion.

*$\mathcal{N}$ -criterion [23, Theorem IV]:* Consider two distinct pairs  $(\kappa, \tau)$  and  $(\gamma, \delta) \in \mathcal{N}_N^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ . A necessary and sufficient condition for  $(\kappa, \tau)$  and  $(\gamma, \delta)$  to be adjacent is that simultaneously

- (i)  $|\kappa\delta - \tau\gamma| = 1$  or  $\sqrt{2}$ ,
- (ii)  $(\kappa + \epsilon\gamma, \tau + \epsilon\delta) \notin \mathcal{N}_N$  for some choice of  $\epsilon = \pm 1$  or  $\pm i$ . ■

### E. Properties and Identification of Adjacent Characteristic Differences

In this part, we put forth three criteria, referred to as the *Q-criteria 1-3*, to identify the adjacency relationships among elements in the  $\mathcal{Q}_q^{char}$ -set. These criteria are analogous to, but not exactly the same as, the  $\mathcal{N}$ -criterion in [23, Theorem IV].

*Q-criterion 1:* Consider two distinct pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ , where  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| = 1$  or  $\sqrt{2}$ . The two pairs are adjacent if and only if  $(\kappa + \epsilon\gamma, \tau + \epsilon\delta) \notin \mathcal{Q}_q$  for some  $\epsilon \in \{\pm 1, \pm i\}$ .

*Proof of Q-criterion 1:* For  $|\Xi| = 1$  or  $\sqrt{2}$ , we simply go through the proof of  $\mathcal{N}$ -criterion in [23, Theorem IV] and verify that after substituting the  $\mathcal{Q}_q^{char}$ -set for the  $\mathcal{N}_N^{char}$ -set, the proof remains valid. ■

The following criterion goes beyond the  $\mathcal{N}$ -criterion in [23] because for the  $\mathcal{Q}_q^{char}$ -set where two distinct pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$  can also be adjacent if  $|\kappa\delta - \tau\gamma| = \sqrt{5}$ .

*Q-criterion 2:* Consider two distinct pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ , where  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| = \sqrt{5}$ .

<sup>2</sup> $\mathcal{N}_N^{char}$  and  $\mathcal{N}_N$  correspond to  $\mathfrak{F}_N$  and  $\mathfrak{G}_N$  in [23] respectively.

- (i) Let  $\epsilon \in \{\pm 1, \pm i\}$ . Among the four possible values for  $\epsilon$ , there exists one and only one value such that  $\kappa + \epsilon\gamma = 0 \pmod{\Xi}$  and  $\tau + \epsilon\delta = 0 \pmod{\Xi}$ ;
- (ii)  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent if and only if for the  $\epsilon \in \{\pm 1, \pm i\}$  that satisfies  $\kappa + \epsilon\gamma = 0 \pmod{\Xi}$  and  $\tau + \epsilon\delta = 0 \pmod{\Xi}$ ,  $(\phi, \psi) \triangleq (\kappa + \epsilon\gamma, \tau + \epsilon\delta) \notin \mathcal{Q}_q$ .

*Proof of Q-criterion 2:* For  $|\Xi| = \sqrt{5}$ ,  $\Xi = v(2+i)$  or  $\Xi = v(2-i)$  where  $v$  is a unit. We focus on  $\Xi = v(2+i)$  (the proof for  $\Xi = v(2-i)$  is similar). We first prove (i). Note that  $2+i$  is a Gaussian prime. Thus,  $\mathbb{Z}[i]/(2+i) = \{0, \pm 1, \pm i\}$  is a field. We write

$$\kappa = \Xi q_\kappa + r_\kappa, \quad (58a)$$

$$\tau = \Xi q_\tau + r_\tau, \quad (58b)$$

$$\gamma = \Xi q_\gamma + r_\gamma, \quad (58c)$$

$$\delta = \Xi q_\delta + r_\delta, \quad (58d)$$

where  $q_x \in \mathbb{Z}[i]$  and  $r_x \in \mathbb{Z}[i]/(2+i) = \{0, \pm 1, \pm i\}$  denote the quotients and remainders, respectively, when  $x$  is divided by  $\Xi = 2+i$ . Given  $|\Xi| = |\kappa\delta - \tau\gamma|$ , we must have  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\Xi}$ . Further, by Lemma 7 (presented later), we have three possibilities:

- (p1)  $r_\kappa = r_\gamma = 0, r_\tau, r_\delta \neq 0$ ;  
 (p2)  $r_\tau = r_\delta = 0, r_\kappa, r_\gamma \neq 0$ ;  
 (p3)  $r_\kappa, r_\tau, r_\gamma, r_\delta \neq 0, r_\kappa r_\gamma^{-1} = r_\tau r_\delta^{-1} \pmod{2+i}$ .

We further write

$$\kappa + \epsilon\gamma = \Xi(q_\kappa + \epsilon q_\gamma) + r_\kappa + \epsilon r_\gamma, \quad (59a)$$

$$\tau + \epsilon\delta = \Xi(q_\tau + \epsilon q_\delta) + r_\tau + \epsilon r_\delta. \quad (59b)$$

In order that  $\kappa + \epsilon\gamma = 0 \pmod{2+i}$  and  $\tau + \epsilon\delta = 0 \pmod{2+i}$ , we must have  $r_\kappa + \epsilon r_\gamma = 0 \pmod{2+i}$  and  $r_\tau + \epsilon r_\delta = 0 \pmod{2+i}$ . If (p1) above applies, we let  $\epsilon = -r_\tau r_\delta^{-1} \pmod{2+i}$ ; if (p2) above applies, we let  $\epsilon = -r_\kappa r_\gamma^{-1} \pmod{2+i}$ ; if (p3) above applies, we let  $\epsilon = -r_\kappa r_\gamma^{-1} = -r_\tau r_\delta^{-1} \pmod{2+i}$ . Note that for all three cases,  $\epsilon \in \{\pm 1, \pm i\}$  and there is only one such  $\epsilon$  that serves the purpose. This proves (i). We next prove (ii).

*“If” part:*  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent if for the  $\epsilon \in \{\pm 1, \pm i\}$  that satisfies  $\kappa + \epsilon\gamma = 0 \pmod{\Xi}$  and  $\tau + \epsilon\delta = 0 \pmod{\Xi}$ ,  $(\phi, \psi) \triangleq (\kappa + \epsilon\gamma, \tau + \epsilon\delta) \notin \mathcal{Q}_q$ .

First, we show that both  $\phi \neq 0$  and  $\psi \neq 0$ . Suppose that  $\phi = \kappa + \epsilon\gamma = 0$ . Then,  $\kappa = -\epsilon\gamma$ . Substituting this into  $\kappa\delta - \tau\gamma$ , we have  $\kappa\delta - \tau\gamma = \gamma(-\epsilon\gamma - \tau)$ , but this contradicts the fact that  $\kappa\delta - \tau\gamma = 2+i$  is a Gaussian prime that cannot be factorized. Thus,  $\phi \neq 0$ . Similarly,  $\psi \neq 0$ . Given that  $\phi = 0 \pmod{\Xi}$  and  $\psi = 0 \pmod{\Xi}$ , and that  $\phi \neq 0$  and  $\psi \neq 0$ , let us define  $(\phi', \psi') \triangleq (\frac{\phi}{\Xi}, \frac{\psi}{\Xi})$ , where  $\phi' \neq 0$  and  $\psi' \neq 0$ . Further, define  $z \triangleq \frac{\phi'}{\psi'}$ .

If  $(\phi, \psi) \notin \mathcal{Q}_q$ , we have  $(\phi', \psi') \notin \mathcal{Q}_q$  and therefore  $\eta = z = \frac{\phi'}{\psi'}$  is not a zero- $l_{\min}$  channel gain (i.e.,  $(\phi', \psi')$  is not a distance-valid difference pair). In the following, we show that there is no other distance-valid difference pair that is closer to  $\eta = z$  than are  $(\kappa, \tau)$  and  $(\gamma, \delta)$  in terms of weighted distance, and that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are equidistant to  $\eta = z$ . In other words,  $\eta = z$  lies on the edge of the Voronoi regions of  $(\kappa, \tau)$  and  $(\gamma, \delta)$ . Thus,  $(\kappa, \tau)$  and  $(\gamma, \delta)$  must be adjacent.

The weighted distances from  $\frac{\kappa}{\tau}$  to  $z$  and  $\frac{\gamma}{\delta}$  to  $z$  are

$$\begin{aligned} |\tau z - \kappa| &= |\delta z - \gamma| = \frac{|\delta\phi' - \gamma\psi'|}{|\psi'|} \\ &= \frac{|\delta\phi - \gamma\psi|/|\Xi|}{|\psi'|} = \frac{1}{|\psi'|}. \end{aligned} \quad (60)$$

where we can verify that  $|\delta\phi - \gamma\psi| = |\Xi|$ .

Now, let us consider any arbitrary  $(a, b) \in \mathcal{Q}_q^{char}$  where  $(a, b) \neq (\kappa, \tau), (\gamma, \delta)$ . Since the normalized distance from  $\frac{a}{b}$  to  $z$  is at least 1, we have

$$|b\phi' - a\psi'| \geq 1 \Rightarrow |b\frac{\phi'}{\psi'} - a| \geq \frac{1}{|\psi'|}. \quad (61)$$

From (60) and (61), the weighted distance from  $\frac{a}{b}$  to  $z$  is not less than  $|\tau z - \kappa| = |\delta z - \gamma| = \frac{1}{|\psi'|}$ . Therefore,  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent in the  $\mathcal{Q}_q^{char}$ -set.

*“Only if” part:*  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent only if for the  $\epsilon \in \{\pm 1, \pm i\}$  that satisfies  $\kappa + \epsilon\gamma = 0 \pmod{\Xi}$  and  $\tau + \epsilon\delta = 0 \pmod{\Xi}$ ,  $(\phi, \psi) = (\kappa + \epsilon\gamma, \tau + \epsilon\delta) \notin \mathcal{Q}_q$ .

Suppose that  $(\phi, \psi) = (\kappa + \epsilon\gamma, \tau + \epsilon\delta) \in \mathcal{Q}_q$ , we want to show that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are not adjacent. Again, as in the proof of the “if” part, we let  $(\phi', \psi') = (\frac{\phi}{\Xi}, \frac{\psi}{\Xi})$ . Note that  $(\phi', \psi') \in \mathcal{Q}_q$  given that  $(\phi, \psi) \in \mathcal{Q}_q$ . Consider the boundary (edge)  $z$  between  $(\kappa, \tau)$  and  $(\gamma, \delta)$  defined by

$$|\tau z - \kappa| = |\delta z - \gamma|. \quad (62)$$

In (63) below, we prove that for any point  $z$  that lies on the boundary as specified in (62),  $|\psi'z - \phi'| < |\tau z - \kappa| = |\delta z - \gamma|$ . In other words,  $(\phi', \psi')$  is closer to  $z$  than are  $(\kappa, \tau)$  and  $(\gamma, \delta)$ , and thus  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are not adjacent.

$$\begin{aligned} |\psi'z - \phi'| &= \frac{|\psi z - \phi|}{|\Xi|} = \frac{|\tau z - \kappa + \epsilon(\delta z - \gamma)|}{|\Xi|} \\ &= |\tau z - \kappa| \frac{|1 + \epsilon(\delta z - \gamma)/(\tau z - \kappa)|}{|\Xi|} \\ &\leq |\tau z - \kappa| \frac{1 + |\epsilon(\delta z - \gamma)/(\tau z - \kappa)|}{|\Xi|} \\ &= |\tau z - \kappa| \frac{1 + 1}{|\Xi|} < |\tau z - \kappa|. \end{aligned} \quad (63)$$

where the last inequality holds because  $|\Xi| = \sqrt{5}$ . ■

An example showing that it is possible for two characteristic differences to be adjacent if their normalized distance is  $\sqrt{5}$  is as follows. Consider the case of  $q = 11$ . Let  $\kappa = 10 + 9i, \tau = 1 - 10i, \gamma = 9 + 8i, \delta = 1 - 9i$ , and  $\epsilon = 1$ . In this case,  $|\Xi| = |\kappa\delta - \tau\gamma| = |2 + i| = \sqrt{5}$ . We can verify that (i) in Q-criterion 2 is satisfied only when  $\epsilon = 1$ , since

$$\begin{aligned} \Xi\phi = \kappa + \epsilon\gamma &\Rightarrow (2+i)(11+3i) = 19+17i, \\ &\Rightarrow \phi = 11+3i, \\ \Xi\psi = \tau + \epsilon\delta &\Rightarrow (2+i)(-3-8i) = 2-19i, \\ &\Rightarrow \psi = -3-8i. \end{aligned} \quad (64)$$

Given (64), we can further verify that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent, since  $(\phi, \psi) = (11+3i, -3-8i) \notin \mathcal{Q}_{11}$ . This can be easily seen as follows. For  $q = 11$ , any valid symbol  $w = w^R + iw^I$  has its real and imaginary parts bounded as  $-5 \leq$

$w^R, w^I \leq 5$ . Thus, the difference between two valid symbols is bounded as  $-10 \leq \delta^R, \delta^I \leq 10$ . Clearly, the real part of  $\phi = 11 + 3i$  does not satisfy this bound.

**Lemma 7:** With respect to the statement of *Q-criterion 2* and the equations as written in (58), given that  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\Xi}$  and  $\gcd(\kappa, \tau) = \gcd(\gamma, \delta) = 1$ , (i) it is not possible for  $r_\kappa = r_\tau = 0$  or  $r_\gamma = r_\delta = 0$ ; (ii) for a Gaussian prime  $\Xi$ , we have  $r_\kappa = 0 \Leftrightarrow r_\gamma = 0$  and  $r_\tau = 0 \Leftrightarrow r_\delta = 0$ .

*Proof of Lemma 7:* (i) is obvious because if  $r_\kappa = r_\tau = 0$ , then from (58),  $\Xi$  is a common factor of  $\kappa$  and  $\tau$ , but this contradicts the fact that  $\gcd(\kappa, \tau) = 1$  given that  $(\kappa, \tau) \in \mathcal{Q}_q^{char}$ . Similarly, it is not possible that  $r_\gamma = r_\delta = 0$ . Therefore, it is not possible for  $r_\kappa = r_\tau = 0$  or  $r_\gamma = r_\delta = 0$ .

For (ii), w.l.o.g., suppose that  $r_\kappa = 0$ , then  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\Xi}$  implies either  $r_\gamma = 0$  or  $r_\tau r_\gamma$  is a non-zero multiple of  $\Xi$  (this later case, however, is not possible because when  $\Xi$  is prime, finite-field arithmetic applies to the remainders. The multiplication of any two nonzero elements of a finite field does not give 0—i.e., it is not congruent to  $\Xi$ ). Thus, we have  $r_\kappa = 0 \Rightarrow r_\gamma = 0$ . By symmetry argument, we thus have  $r_\kappa = 0 \Leftarrow r_\gamma = 0$ . Similarly, we have  $r_\tau = 0 \Leftrightarrow r_\delta = 0$ . ■

**Q-criterion 3:** Consider two distinct pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| \neq 1, \sqrt{2}$  or  $\sqrt{5}$ . The two pairs are not adjacent.

*Proof of Q-criterion 3:* The proof of *Q-criterion 3* is given by a series of lemmas. As we will show by the following lemmas,  $(\kappa, \tau), (\gamma, \delta)$  are not adjacent if

- $|\Xi| \geq 40$  by *Lemmas 8* and *8.1*;
- $|\Xi| = \sqrt{13}, \sqrt{17}, \sqrt{2}\sqrt{13}, \sqrt{29}, \sqrt{2}\sqrt{17}$ , or  $\sqrt{37}$  by *Lemmas 8* and *8.2*;
- $|\Xi| = \sqrt{10}$  and  $\sqrt{2}\sqrt{10}$  by *Lemmas 8* and *8.3*;
- $|\Xi| = 5$  by *Lemmas 8* and *8.4*;
- $|\Xi| = 2, 2\sqrt{2}, 3, 2 \cdot 2, 3\sqrt{2}, 2\sqrt{8}$ , or  $2 \cdot 3$  by *Lemma 10*. ■

**Lemma 8 (A modified version of Lemma 4 in [23]):**

Consider two distinct  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $\Xi \triangleq \kappa\delta - \tau\gamma$  contains a factor  $\tilde{\Xi}$ . The two pairs are not adjacent if there exist  $(\zeta, \vartheta), (\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$  such that

$$\kappa\zeta + \gamma\vartheta = \tilde{\Xi}\phi, \quad (65a)$$

$$\tau\zeta + \delta\vartheta = \tilde{\Xi}\psi, \quad (65b)$$

$$0 < |\zeta| + |\vartheta| \leq \frac{|\tilde{\Xi}|}{\sqrt{2}}. \quad (65c)$$

*Proof of Lemma 8:* Suppose that  $|\Xi| \neq 1, \sqrt{2}$  or  $\sqrt{5}$ , but  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent. According to (65a), we have

$$\begin{aligned} |\phi| &= \left| \frac{\kappa\zeta + \gamma\vartheta}{\tilde{\Xi}} \right| \leq \frac{|\zeta| + |\vartheta|}{|\tilde{\Xi}|} \max\{|\kappa|, |\gamma|\} \\ &\leq \frac{1}{\sqrt{2}} \max\{|\kappa|, |\gamma|\} \leq \frac{\sqrt{2|q|^2 - 4q^R + 2}}{\sqrt{2}} < |q|. \end{aligned} \quad (66)$$

where the second inequality holds due to (65b) and the third equality is due to *Lemma 2*. Similarly, we have  $|\psi| < |q|$ . Therefore, by *Lemma 3*, we have  $(\phi, \psi) \in \mathcal{Q}_q$ .

Now, if  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent, then from (55), there exists a common point  $z'$  equidistant to  $(\kappa, \tau)$  and  $(\gamma, \delta)$  such that no other generators are closer to  $z'$  than are  $(\kappa, \tau)$  and  $(\gamma, \delta)$ . Let us compute the weighted distance from  $(\phi, \psi)$  to  $z'$ :

$$\begin{aligned} |\psi z' - \phi| &= \frac{|\zeta(\tau z' - \kappa) + \vartheta(\delta z' - \gamma)|}{|\tilde{\Xi}|} \\ &\leq \frac{|\zeta(\tau z' - \kappa)| + |\vartheta(\delta z' - \gamma)|}{|\tilde{\Xi}|} \\ &\leq \frac{|\zeta| + |\vartheta|}{|\tilde{\Xi}|} \max\{|\tau z' - \kappa|, |\delta z' - \gamma|\} \\ &\leq \frac{|\tau z' - \kappa|}{\sqrt{2}} < |\tau z' - \kappa|. \end{aligned} \quad (67)$$

Obviously, (67) contradicts our assumption that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent. ■

**Lemma 8.1:** Consider two distinct  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| \geq 40$ . There exist  $(\zeta, \vartheta), (\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$  such that

$$\kappa\zeta + \gamma\vartheta = \Xi\phi, \quad (68a)$$

$$\tau\zeta + \delta\vartheta = \Xi\psi, \quad (68b)$$

$$0 < |\zeta| + |\vartheta| \leq \frac{|\Xi|}{\sqrt{2}}. \quad (68c)$$

*Proof of Lemma 8.1:* If we write  $\zeta = \zeta^R + i\zeta^I$  and  $\vartheta = \vartheta^R + i\vartheta^I$  where  $\zeta^R, \zeta^I, \vartheta^R, \vartheta^I$  are real, then  $(\zeta^R, \zeta^I, \vartheta^R, \vartheta^I)^T$  that satisfy (68a) and (68b) form a four-dimensional lattice  $\Lambda$  of determinant  $d(\Lambda) = |\Xi|^2$ , as explained below.

Let us represent Gaussian integers in (68a) by  $2 \times 2$  matrices and  $2 \times 1$  vectors. Specifically, we rewrite (68a) as

$$\begin{pmatrix} \kappa & \gamma \\ \tau & \delta \end{pmatrix} \begin{pmatrix} \zeta \\ \vartheta \end{pmatrix} = \begin{pmatrix} \Xi & 0 \\ 0 & \Xi \end{pmatrix} \begin{pmatrix} \phi \\ \psi \end{pmatrix}, \quad (69)$$

where

$$\begin{aligned} \kappa &= \begin{pmatrix} \kappa^R & -\kappa^I \\ \kappa^I & \kappa^R \end{pmatrix}, \gamma = \begin{pmatrix} \gamma^R & -\gamma^I \\ \gamma^I & \gamma^R \end{pmatrix}, \\ \tau &= \begin{pmatrix} \tau^R & -\tau^I \\ \tau^I & \tau^R \end{pmatrix}, \delta = \begin{pmatrix} \delta^R & -\delta^I \\ \delta^I & \delta^R \end{pmatrix}, \\ \Xi &= \begin{pmatrix} \Xi^R & -\Xi^I \\ \Xi^I & \Xi^R \end{pmatrix} = \kappa\delta - \tau\gamma, \zeta = \begin{pmatrix} \zeta^R \\ \zeta^I \end{pmatrix}, \\ \vartheta &= \begin{pmatrix} \vartheta^R \\ \vartheta^I \end{pmatrix}, \phi = \begin{pmatrix} \phi^R \\ \phi^I \end{pmatrix}, \psi = \begin{pmatrix} \psi^R \\ \psi^I \end{pmatrix}. \end{aligned} \quad (70)$$

Multiplying both sides of (69) by  $\begin{pmatrix} \Xi^{-1} & 0 \\ 0 & \Xi^{-1} \end{pmatrix}$ , we get

$$\begin{pmatrix} \zeta \\ \vartheta \end{pmatrix} = \begin{pmatrix} \Xi^{-1} & 0 \\ 0 & \Xi^{-1} \end{pmatrix} \begin{pmatrix} \delta & -\gamma \\ -\tau & \kappa \end{pmatrix} \begin{pmatrix} \Xi & 0 \\ 0 & \Xi \end{pmatrix} \begin{pmatrix} \phi \\ \psi \end{pmatrix}. \quad (71)$$

Thus, we see that  $\begin{pmatrix} \zeta \\ \vartheta \end{pmatrix}$  form a four-dimensional lattice

$\Lambda$  with determinant

$$\begin{aligned} \det \left( \begin{pmatrix} \Xi^{-1} & \mathbf{0} \\ \mathbf{0} & \Xi^{-1} \end{pmatrix} \begin{pmatrix} \delta & -\gamma \\ -\tau & \kappa \end{pmatrix} \begin{pmatrix} \Xi & \mathbf{0} \\ \mathbf{0} & \Xi \end{pmatrix} \right) \\ = \det \left( \begin{pmatrix} \Xi^{-1} & \mathbf{0} \\ \mathbf{0} & \Xi^{-1} \end{pmatrix} \right) \det \left( \begin{pmatrix} \delta & -\gamma \\ -\tau & \kappa \end{pmatrix} \right) \det \left( \begin{pmatrix} \Xi & \mathbf{0} \\ \mathbf{0} & \Xi \end{pmatrix} \right) \\ = \det \left( \begin{pmatrix} \delta & -\gamma \\ -\tau & \kappa \end{pmatrix} \right) = \det(\kappa\delta - \tau\gamma) = \det(\Xi) = |\Xi|^2. \end{aligned} \quad (72)$$

Next, to prove the validity of (68b), we have to show the existence of a lattice point other than  $(0, 0, 0, 0)$  in the convex region  $\mathcal{G}$  as defined below:

$$\mathcal{G} \triangleq \{(\zeta^R, \zeta^I, \vartheta^R, \vartheta^I) \in \mathbb{R}^4 \mid \sqrt{(\zeta^R)^2 + (\zeta^I)^2} + \sqrt{(\vartheta^R)^2 + (\vartheta^I)^2} \leq \frac{|\Xi|}{\sqrt{2}}\}. \quad (73)$$

Note that the zero lattice point  $(\zeta^R, \zeta^I, \vartheta^R, \vartheta^I) = (0, 0, 0, 0)$  is not acceptable because of the statement of the lemma that  $|\zeta| + |\vartheta| > 0$ ; on the other hand, a non-zero lattice point of  $(\zeta^R, \zeta^I, \vartheta^R, \vartheta^I)$  automatically yields a non-zero solution for  $(\phi^R, \phi^I, \psi^R, \psi^I)$  according to (69).

The volume of  $\mathcal{G}$  is given by

$$\mathcal{V}(\mathcal{G}) = \int_{(\zeta^R, \zeta^I, \vartheta^R, \vartheta^I) \in \mathcal{G}} d\zeta^R d\zeta^I d\vartheta^R d\vartheta^I. \quad (74)$$

By change of rectangular coordinate systems of  $(\zeta^R, \zeta^I)$  and  $(\vartheta^R, \vartheta^I)$  to polar coordinate systems, where  $r = \sqrt{(\zeta^R)^2 + (\zeta^I)^2}$  and  $r' = \sqrt{(\vartheta^R)^2 + (\vartheta^I)^2}$ , we can rewrite (74) as

$$\begin{aligned} \mathcal{V}(\mathcal{G}) &= \int_{r=0}^{\frac{|\Xi|}{\sqrt{2}}} \int_{r'=0}^{\frac{|\Xi|}{\sqrt{2}}-r} (2\pi r)(2\pi r') dr' dr \\ &= \int_{r=0}^{\frac{|\Xi|}{\sqrt{2}}} (2\pi r) \left( \pi \left( \frac{|\Xi|}{\sqrt{2}} - r \right)^2 \right) dr = \frac{\pi^2 |\Xi|^4}{24}. \end{aligned} \quad (75)$$

By *Minkowski's Convex Body Theorem* [24], there is a lattice point other than  $(0, 0, 0, 0)$  in  $\mathcal{G}$  if

$$\mathcal{V}(\mathcal{G}) > 2^4 d(\Lambda). \quad (76)$$

That is,  $\frac{\pi^2 |\Xi|^4}{24} > 2^4 |\Xi|^2$  or  $|\Xi|^2 > \frac{384}{\pi^2} \approx 38.9$ . Therefore, we have proved the lemma for  $|\Xi|^2 \geq 40$ . ■

*Lemmas 8 and 8.1* cover the cases with normalized distances  $|\Xi| = |\kappa\delta - \tau\gamma| \geq \sqrt{40}$ . There are 16 remaining cases of  $\Xi$  when  $|\Xi|^2 \neq 1, 2$ , or 5 and  $|\Xi|^2 < 40$  as follows:

$$\begin{aligned} |\Xi|^2 &= 4, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37. \\ \text{i.e., } |\Xi| &= 2, 2\sqrt{2}, 3, \sqrt{10}, \sqrt{13}, 2 \cdot 2, \sqrt{17}, 3\sqrt{2}, \sqrt{2}\sqrt{10}, 5, \\ &\sqrt{2}\sqrt{13}, \sqrt{29}, 2\sqrt{8}, \sqrt{2}\sqrt{17}, 2 \cdot 3, \sqrt{37}. \end{aligned}$$

*Lemma 8.2:* Consider two distinct  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $\Xi \triangleq \kappa\delta - \tau\gamma$  contains a factor  $\tilde{\Xi}$  with magnitude  $|\tilde{\Xi}| = \sqrt{13}, \sqrt{17}, \sqrt{29}, \sqrt{37}$ . There exist  $(\zeta, \vartheta), (\phi, \psi) \in$

$\mathbb{Z}^2[i] \setminus \{(0, 0)\}$  such that

$$\kappa\zeta + \gamma\vartheta = \tilde{\Xi}\phi, \quad (77a)$$

$$\tau\zeta + \delta\vartheta = \tilde{\Xi}\psi, \quad (77b)$$

$$0 < |\zeta| + |\vartheta| \leq \frac{|\tilde{\Xi}|}{\sqrt{2}}. \quad (77c)$$

*Remark:* All these  $\tilde{\Xi}$  are complex Gaussian-integer primes.

*Proof of Lemma 8.2:* The proof is given in Appendix IV. ■

*Lemmas 8 and 8.2* cover the cases with normalized distances  $|\Xi| = \sqrt{13}, \sqrt{17}, \sqrt{2}\sqrt{13}, \sqrt{29}, \sqrt{2}\sqrt{17}, \sqrt{37}$ . The remaining cases are

$$|\Xi| = 2, 2\sqrt{2}, 3, \sqrt{10}, 2 \cdot 2, 3\sqrt{2}, \sqrt{2}\sqrt{10}, 5, 2\sqrt{8}, 2 \cdot 3. \quad (78)$$

*Lemma 8.3:* Consider two distinct  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $\Xi \triangleq \kappa\delta - \tau\gamma$  contains a factor  $\tilde{\Xi}$  with magnitude  $|\tilde{\Xi}| = \sqrt{10}$ . There exist  $(\zeta, \vartheta), (\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$  such that

$$\kappa\zeta + \gamma\vartheta = \tilde{\Xi}\phi, \quad (79a)$$

$$\tau\zeta + \delta\vartheta = \tilde{\Xi}\psi, \quad (79b)$$

$$0 < |\zeta| + |\vartheta| \leq \frac{|\tilde{\Xi}|}{\sqrt{2}}. \quad (79c)$$

*Proof of Lemma 8.3:* The proof is given in Appendix V. ■

*Lemmas 8 and 8.3* cover the cases with normalized distances  $|\Xi| = \sqrt{10}, \sqrt{2}\sqrt{10}$ . The remaining cases are

$$|\Xi| = 2, 2\sqrt{2}, 3, 2 \cdot 2, 3\sqrt{2}, 5, 2\sqrt{8}, 2 \cdot 3.$$

*Lemma 8.4:* Consider two distinct  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $\Xi \triangleq \kappa\delta - \tau\gamma = 5$ . There exist  $(\zeta, \vartheta), (\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$  such that

$$\kappa\zeta + \gamma\vartheta = \Xi\phi, \quad (80a)$$

$$\tau\zeta + \delta\vartheta = \Xi\psi, \quad (80b)$$

$$0 < |\zeta| + |\vartheta| \leq \frac{|\Xi|}{\sqrt{2}}. \quad (80c)$$

*Proof of Lemma 8.4:* The proof is given in Appendix VI. ■

*Lemmas 8 and 8.4* cover the case with normalized distance  $|\Xi| = 5$ . The remaining cases are  $|\Xi| = 2, 2\sqrt{2}, 3, 2 \cdot 2, 3\sqrt{2}, 2\sqrt{8}, 2 \cdot 3$ .

In the following, we introduce the concept of convex region for the set of valid differences.

*Definition 13:* Given a Gaussian prime  $q$ , we have defined  $\Lambda$  (see *Definition 5*) as a set of Gaussian integers that collects all valid differences (see Fig. 10). Given this  $\Lambda$ , we can form a closed convex region  $\mathcal{G}_q$  on the complex plane, defined by

$$\begin{aligned} \mathcal{G}_q &\triangleq \{g \in \mathbb{C} \mid g = \sum_{\delta_i \in \Lambda} a_i \delta_i, \\ &\text{where } a_i \in \mathbb{R}, 0 \leq \forall a_i \leq 1, \text{ and } \sum_i a_i = 1\}. \end{aligned} \quad (81)$$



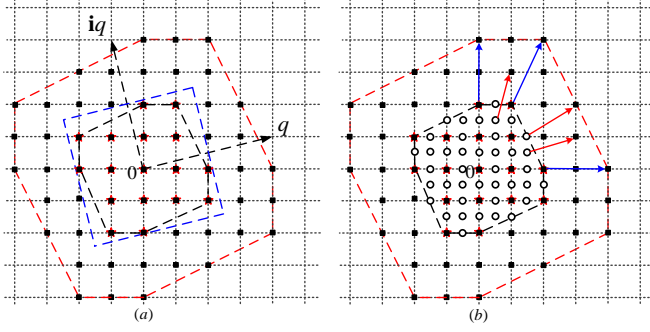


Fig. 10. Valid differences of  $q = 4 + i$  and convex region formed by the differences, where red stars are  $\mathbb{Z}[i]/q$  and the black squares are distance-valid differences. (a) Gaussian integers within the blue square are elements of  $\mathbb{Z}[i]/q$ , and the inner octagon in black dashed line denotes the convex region formed by elements in  $\mathbb{Z}[i]/q$ ; (b) circles and red stars within the convex region of  $\mathbb{Z}[i]/q$  (inner octagon) are valid differences scaled by half (i.e., the lattice points in the outer octagon scaled by half).

Given Definition 13, we have a lemma as follows:

**Lemma 9:** Any Gaussian integer within the convex region  $\mathcal{G}_q$  is a valid difference.

*Proof of Lemma 9:*

A sketch of the proof is as follows. With reference to the example with  $q = 4 + i$  in Fig. 10, we can define the convex region formed by valid symbols in  $\mathbb{Z}[i]/q$  (see the inner octagon in black dashed line; note that for the case of a real  $q$ , the convex region will be a square rather than an octagon) as

$$\{x \in \mathbb{C} | x = \sum_{i=1}^{|q|^2} a_i w_i, \text{ where } a_i \in \mathbb{R}, 0 \leq \forall a_i \leq 1, \sum_{i=1}^{|q|^2} a_i = 1, \text{ and } \forall w_i \in \mathbb{Z}[i]/q\}. \quad (82)$$

Note that the convex region formed by the valid differences,  $\mathcal{G}_q$ , (see the outer octagon in red dashed line in Fig. 10) is a scaled-up version of this convex region. The scaled-up factor is 2. We need to prove that every Gaussian integer (black squares in Fig. 10(a)) within  $\mathcal{G}_q$  is a scaled-up point induced by two Gaussian integers (red stars in Fig. 10(a)) in  $\mathbb{Z}[i]/q$ . In other words, we can express any lattice point  $\delta$  in  $\mathcal{G}_q$  as  $\delta = w - w'$ , where  $w, w' \in \mathbb{Z}[i]/q$ .

We introduce the concept of *scaled-by-half* lattice as follows: a scaled-by-half lattice is  $\frac{1}{2}\mathbb{Z}[i]$ , where  $z' \in \frac{1}{2}\mathbb{Z}[i]$  if and only if  $z' = \frac{1}{2}z$ , for some  $z \in \mathbb{Z}[i]$ . The set of valid symbols is  $\mathcal{W} = \mathbb{Z}[i]/q$ . We define  $\tilde{\mathcal{W}} = \frac{1}{2}\mathcal{W} = \frac{1}{2}\mathbb{Z}[i]/q$ . With respect to Fig. 10, the lattice points within the inner octagon in Fig. 10(a) (red stars) are  $\mathcal{W}$ , and the lattice points within the inner octagon in Fig. 10(b) (white circles and red stars) are  $\tilde{\mathcal{W}}$ . Note that  $\mathcal{W} \subset \tilde{\mathcal{W}}$ .

Denote a Gaussian integer in the outer octagon whose real and imaginary parts are both even by  $\delta_e$ . We note that each  $\delta_e$  is a scaled-up-by-2 version of a  $w \in \mathcal{W}$  (see the blue solid lines with arrow in Fig. 10(b)). There is a one-to-one mapping between the points in  $\mathcal{W}$  and the set of Gaussian integers  $\delta_e$ .

For such a Gaussian integer, we can write

$$\delta_e = 2w = w + w, \text{ for some } w \in \mathcal{W}. \quad (83)$$

We note that since  $\mathcal{W}$  is a field, and therefore each element in  $\mathcal{W}$  has an additive inverse, and each element is an additive inverse of some other element. Specifically,  $w \in \mathcal{W}$  is the inverse of some  $w' \in \mathcal{W}$ . We can thus write

$$\delta_e = 2w = w - w', \text{ where both } w, w' \in \mathcal{W}. \quad (84)$$

Denote a Gaussian integer in the outer octagon whose real and imaginary parts are not both even by  $\delta_o$ . We note that each  $\delta_o$  is a scaled-up-by-2 version of a  $\tilde{w} \in \tilde{\mathcal{W}} \setminus \mathcal{W}$  (see the red solid lines with arrow in Fig. 10 (b)). We further note that for any  $\tilde{w} \in \tilde{\mathcal{W}} \setminus \mathcal{W}$ , we can write  $\tilde{w} = \frac{1}{2}w + \frac{1}{2}w'$ , for some  $w, w' \in \mathcal{W}$  (i.e.,  $\tilde{w}$  is an equal-weight linear combination of two valid symbols in  $\mathcal{W}$ ). Thus,  $\delta_o$  can be expressed as

$$\delta_o = w + w', \text{ where both } w, w' \in \mathcal{W}. \quad (85)$$

Again,  $w'$  is the inverse of some  $w'' \in \mathcal{W}$  and vice versa, giving  $\delta_o = w - w''$ .

Thus, for any Gaussian integer  $\delta$  within the convex region  $\mathcal{G}_q$ , we can find two  $w, w' \in \mathbb{Z}[i]/q$  such that  $\delta = w - w'$ . This completes the proof. ■

**Lemma 10:** Consider two distinct  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$ ,  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$ , and that  $\Xi \triangleq \kappa\delta - \tau\gamma$  contains a factor  $\tilde{\Xi}$  with magnitude  $|\tilde{\Xi}| = 2$  or 3. The two pairs  $(\kappa, \tau), (\gamma, \delta)$  are non-adjacent.

*Proof of Lemma 10:* The proof is given in Appendix VII. ■

Lemma 10 covers the cases with normalized distances  $|\Xi| = 2, 2\sqrt{2}, 3, 2 \cdot 2, 3\sqrt{2}, 2\sqrt{8}, 2 \cdot 3$ .

#### F. $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ Analysis Within the Voronoi Region

Given an arbitrary characteristic difference  $(\delta_A^{char}, \delta_B^{char})$ , Part E has given a set of criteria for the identification of its adjacent characteristic differences. In this part, we prove (T4-1) and (T4-2) stated at the end of Part C. First, we use these criteria to prove (T4-1), restated as Lemma 11 below.

**Lemma 11 (T4-1):** Two distinct characteristic differences  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  (i.e.,  $(\delta_A^{char}, \delta_B^{char}) \neq \nu(\delta_A^{char'}, \delta_B^{char'}), \forall \nu \in \{\pm 1, \pm i\}$ ) that are adjacent cannot be clustered by the same NC mapping.

*Proof of Lemma 11:* Given  $(\delta_A^{char}, \delta_B^{char}), (\delta_A^{char'}, \delta_B^{char'}) \in \mathcal{Q}_q^{char}$ , if  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  are adjacent, the adjacent pair yields  $|\Xi| = |\delta_B^{char} \delta_A^{char'} - \delta_A^{char} \delta_B^{char'}| = 1, \sqrt{2}$ , or  $\sqrt{5}$  by Q-criteria 1-3. Furthermore,  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  are clustered by the same NC mapping if and only if  $\delta_B^{char(q)} \delta_A^{char(q)'} - \delta_A^{char(q)} \delta_B^{char(q)'} = 0 \pmod{q}$ .

**Case 1:**  $|q| = \sqrt{2}$

Consider a Gaussian prime  $q$  with  $|q| = \sqrt{2}$  (e.g.,  $q = 1 + i$ ). In this case, we have four zero- $l_{\min}$  gains in the complex plane of  $\eta$ : two non-trivial zero- $l_{\min}$  channel gains, i.e.,  $\eta^o = 1$  and  $-1$ , associated with  $(\delta_A^{char}, \delta_B^{char}) = (1, -1)$  and  $(1, 1)$  respectively, and two trivial zero- $l_{\min}$  channel gains  $\eta^o = 0$

and  $\eta^o = \infty$ , associated with  $(\delta_A^{char}, \delta_B^{char}) = (1, 0)$  and  $(0, 1)$  respectively. For  $|q| = \sqrt{2}$ , we can prove *Lemma 11* by considering the adjacent Voronoi regions of each characteristic difference. For example, at  $\eta^o = -1$  associated with  $(\delta_A^{char}, \delta_B^{char}) = (1, 1)$ , the adjacent characteristic difference is  $(\delta_A^{char'}, \delta_B^{char'}) = (1, 0)$  by *Q-criterion 1* (note that the Voronoi regions of  $\eta^o = 1$  and  $-1$  are not adjacent), and  $(\delta_A^{char'}, \delta_B^{char'})$  cannot be clustered by any NC mapping.

**Case 2:**  $|q| \geq \sqrt{5}$

Consider a Gaussian prime  $q$  with  $|q| \geq \sqrt{5}$ . In the following, we verify that it is not possible to have

$$\Xi \triangleq \delta_B^{char} \delta_A^{char'} - \delta_A^{char} \delta_B^{char'} = mq, \quad m \in \mathbb{Z}[i], \quad (86)$$

(i.e., not possible to have  $\delta_B^{char(q)} \delta_A^{char(q)'} - \delta_A^{char(q)} \delta_B^{char(q)'} = 0 \pmod{q}$ ), if  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  satisfy *Q-criteria 1-3*.

For  $|\Xi| = 1$  (i.e.,  $\Xi \in \{\pm 1, \pm i\}$ ), (86) is not possible because it is not possible to have  $1 = mq, \forall m \in \mathbb{Z}[i]$ .

For  $|\Xi| = \sqrt{2}$  (i.e.,  $\Xi \in v(1+i)$  and  $v \in \{\pm 1, \pm i\}$ ), w.l.o.g., let us consider  $\Xi = 1+i$ . It is not possible to satisfy (86) either because  $1+i \neq mq, \forall m \in \mathbb{Z}[i]$ , since  $1+i$  is prime and cannot be factorized.

For  $|\Xi| = \sqrt{5}$  (i.e.,  $\Xi \in \{v(1+i), v(1+2i)\}$  and  $v \in \{\pm 1, \pm i\}$ ), w.l.o.g., let us consider  $\Xi = 2+i$ . First, let us consider  $|q| > \sqrt{5}$ . In this case, (86) cannot be satisfied because  $\Xi = 2+i \neq mq, \forall m \in \mathbb{Z}[i]$ , since  $2+i$  is prime and cannot be factorized.

Next, consider  $|q| = \sqrt{5}$ . In the following, we show that even though (86) is satisfied,  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  are not adjacent if  $|\Xi| = \sqrt{5}$  (i.e., for  $|q| = \sqrt{5}$ , two difference pairs with a normalized distance of  $\sqrt{5}$  can never be adjacent; it is only when  $|q| \neq \sqrt{5}$  that it is possible for two difference pairs separated by a normalized distance of  $\sqrt{5}$  to be adjacent). W.l.o.g., consider  $q = 2+i$  (the representative elements of  $\mathbb{Z}[i]/(2+i)$  and  $\mathbb{Z}[i]/(2-i)$  are the same). In this case, the valid symbols are  $\{0, \pm 1, \pm i\}$ , and  $\delta_A^{char}, \delta_B^{char}, \delta_A^{char'}, \delta_B^{char'} \in \{0, \pm 1, \pm i, \pm 2, \pm 2i, \pm(1+i), \pm(1-i)\}$ . Let us consider  $\Xi = 2+i$  (similar proof applies for  $\Xi = 2-i$ ).

By (i) in *Q-criterion 2*, there exists one and only one  $\epsilon \in \{\pm 1, \pm i\}$  such that

$$\begin{aligned} \delta_A^{char} + \epsilon \delta_A^{char'} &= 0 \pmod{\Xi}, \\ \delta_B^{char} + \epsilon \delta_B^{char'} &= 0 \pmod{\Xi}. \end{aligned} \quad (87)$$

To satisfy (87), given  $\delta_A^{char}, \delta_B^{char}, \delta_A^{char'}, \delta_B^{char'} \in \{0, \pm 1, \pm i, \pm 2, \pm 2i, \pm(1+i), \pm(1-i)\}$ , we can verify that the values that can be adopted by  $\delta_A^{char} + \epsilon \delta_A^{char'}$  and  $\delta_B^{char} + \epsilon \delta_B^{char'}$  while satisfying (87) must be from the set  $\{0, v(2+i), v(1+i)(2+i)\}$ , where  $v$  is a unit. Furthermore, it is not possible to have  $\delta_A^{char} + \epsilon \delta_A^{char'} = a(2+i)$  or  $\delta_B^{char} + \epsilon \delta_B^{char'} = a(2+i)$  where  $|a| > \sqrt{2}$ . In the following, we list all the possible solutions of (87):

$$(s1) \quad (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (0, 0)$$

It is not possible to have (s1), since for  $(\delta_A^{char}, \delta_B^{char}) \neq v(\delta_A^{char'}, \delta_B^{char'})$ ,  $\forall v \in \{\pm 1, \pm i\}$ , according to the statement of lemma (i.e., the two characteristic differences are distinct).

$$(s2) \quad (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) \neq (0, 0)$$

$$\begin{aligned} (s2-i) \quad & (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (0, v(2+i)) \text{ or } (v(2+i), 0) \\ (s2-ii) \quad & (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (0, v(1+i)(2+i)) = (0, v(1+3i)) \text{ or } (v(1+3i), 0) \\ (s2-iii) \quad & (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (v(2+i), v(2+i)) \\ (s2-iv) \quad & (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (v(2+i), v(1+i)(2+i)) \text{ or } (v(1+i)(2+i), v(2+i)) \\ (s2-v) \quad & (\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (v(1+i)(2+i), v(1+i)(2+i)) \end{aligned}$$

According to the definition of the  $\mathcal{Q}_q$ -set in (54),  $(\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) \in \mathcal{Q}_q$  for all subcases in (s2) above, since each belongs to  $\mathcal{Q}_q^{char}$  after factoring of the gcd (e.g., for  $(\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (0, v(2+i))$ , after factoring out the gcd of  $2+i$  we have  $\frac{1}{2+i}(\delta_A^{char} + \epsilon \delta_A^{char'}, \delta_B^{char} + \epsilon \delta_B^{char'}) = (0, v) \in \mathcal{Q}_q^{char}$ ). According to (ii) in *Q-criterion 2*, therefore, for  $|\Xi| = \sqrt{5}$ ,  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  cannot be adjacent. ■

In the following, we prove (T4-2) by *Lemmas 12-14* and *Corollary 1*.

**Lemma 12:** Consider two non-adjacent pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$  with normalized distance  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| > \sqrt{5}$ . There exists another pair  $(\gamma', \delta') \in \mathcal{Q}_q^{char}$  such that  $|\delta'\eta - \gamma'| < |\delta\eta - \gamma|, \forall \eta \in \mathcal{V}(\frac{\kappa}{\tau})$  and that  $|\Xi'| \triangleq |\kappa\delta' - \tau\gamma'| < |\Xi|$ .

**Remark:** The case of  $|\Xi| = 1, \sqrt{2}, \sqrt{5}$  will be treated separately in *Lemmas 13* and *14*. Note that  $(\gamma', \delta')$  may still be non-adjacent to  $(\kappa, \tau)$ , but the normalized distance with  $(\kappa, \tau)$  is getting smaller.

**Proof of Lemma 12:** If  $|\Xi| > \sqrt{5}$  and  $|\Xi| \neq 2, 3$ , by *Lemmas 8.1-8.4*, there exist  $(\zeta, \vartheta), (\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$ , such that  $\phi = \frac{\zeta\kappa + \vartheta\gamma}{\Xi}, \psi = \frac{\zeta\tau + \vartheta\delta}{\Xi}$  and  $0 < |\zeta| + |\vartheta| \leq \frac{|\Xi|}{\sqrt{2}}$ . Using similar argument as (66), we conclude that  $(\phi, \psi) \in \mathcal{Q}_q$ . Note that it is possible for  $\gcd(\phi, \psi) > 1$ , in which case we can reduce  $(\phi, \psi)$  further to  $(\gamma', \delta') \triangleq (\frac{\phi}{\gcd(\phi, \psi)}, \frac{\psi}{\gcd(\phi, \psi)}) \in \mathcal{Q}_q^{char}$ . Consider an arbitrary  $\eta \in \mathcal{V}(\frac{\kappa}{\tau})$ . Following (67), we write (note: in (67),  $z'$  is a point equidistant to  $(\kappa, \tau)$  and  $(\gamma, \delta)$ ; here,  $\eta$  is not equidistant to  $(\kappa, \tau)$  and  $(\gamma, \delta)$ )

$$\begin{aligned} |\delta'\eta - \gamma'| &\leq |\psi\eta - \phi| = \frac{|\zeta(\tau\eta - \kappa) + \vartheta(\delta\eta - \gamma)|}{|\Xi|} \\ &\leq \frac{|\zeta(\tau\eta - \kappa)| + |\vartheta(\delta\eta - \gamma)|}{|\Xi|} \\ &\leq \frac{|\zeta| + |\vartheta|}{|\Xi|} \max\{|\tau\eta - \kappa|, |\delta\eta - \gamma|\} \\ &\leq \frac{|\delta\eta - \gamma|}{\sqrt{2}} < |\delta\eta - \gamma|, \end{aligned} \quad (88)$$

where the first inequality in the last line holds because  $0 < |\zeta| + |\vartheta| \leq \frac{|\Xi|}{\sqrt{2}}$  and  $|\tau\eta - \kappa| \leq |\delta\eta - \gamma|$  for  $\forall \eta \in \mathcal{V}(\frac{\kappa}{\tau})$ .

Furthermore, we have

$$\begin{aligned} |\Xi'| &\triangleq |\kappa\delta' - \tau\gamma'| \leq |\kappa\psi - \tau\phi| \\ &= \frac{|\kappa(\tau\zeta + \delta\vartheta) - \tau(\kappa\zeta + \gamma\vartheta)|}{|\Xi|} \\ &= \frac{|\vartheta(\kappa\delta - \tau\gamma)|}{|\Xi|} = |\vartheta| \leq \frac{|\Xi|}{\sqrt{2}} < |\Xi|. \end{aligned} \quad (89)$$

If  $|\Xi| = 2$  or  $3$ , by Lemma 10, there exist  $(\zeta, \vartheta), (\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$ , such that  $\phi = \frac{\zeta\kappa + \vartheta\gamma}{\Xi}$  and  $\psi = \frac{\zeta\tau + \vartheta\delta}{\Xi}$ . We consider  $|\Xi| = 2$  only, and the proof for  $|\Xi| = 3$  follows similarly. From the proof of Lemma 10, we have

$$\kappa\zeta + \gamma\vartheta = 2\phi, \quad (90a)$$

$$\tau\zeta + \delta\vartheta = 2\psi, \quad (90b)$$

where both  $\zeta, \vartheta$  are units and both signs of  $\zeta$  satisfy (90).

Then, we rewrite (88) as

$$\begin{aligned} |\delta'\eta - \gamma'| &\leq |\psi\eta - \phi| = \frac{|\zeta(\tau\eta - \kappa) + \vartheta(\delta\eta - \gamma)|}{2} \\ &< \frac{|\zeta(\tau\eta - \kappa)| + |\vartheta(\delta\eta - \gamma)|}{2} \\ &< \frac{|\zeta| + |\vartheta|}{2} \max\{|\tau\eta - \kappa|, |\delta\eta - \gamma|\} \\ &< |\delta\eta - \gamma|, \end{aligned} \quad (91)$$

where we can find a proper sign of  $\zeta$  to validate the second strict inequality. Then, we further have

$$\begin{aligned} |\Xi'| &\triangleq |\kappa\delta' - \tau\gamma'| \leq |\kappa\psi - \tau\phi| \\ &= \frac{|\vartheta(\kappa\delta - \tau\gamma)|}{|\Xi|} = |\vartheta| = 1 < 2. \end{aligned} \quad (92)$$

**Lemma 13:** Consider two non-adjacent pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$  with normalized distance  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| = \sqrt{5}$ . There exists another pair  $(\gamma', \delta') \in \mathcal{Q}_q^{char}$  such that  $|\delta'\eta - \gamma'| < |\delta\eta - \gamma|, \forall \eta \in \mathcal{V}(\frac{\kappa}{\tau})$  and that  $|\Xi'| \triangleq |\kappa\delta' - \tau\gamma'| = 1$ .

*Proof of Lemma 13:* We follow the proof of  $\mathcal{Q}$ -criterion 2. According to (i) of  $\mathcal{Q}$ -criterion 2, there exist one and only one unit  $\epsilon \in \{\pm 1, \pm i\}$  such that  $\kappa + \epsilon\gamma = 0 \pmod{\Xi}$  and  $\tau + \epsilon\delta = 0 \pmod{\Xi}$  for  $|\Xi| = \sqrt{5}$ . Under this  $\epsilon$ , define  $\phi \triangleq \frac{\kappa + \epsilon\gamma}{\Xi}, \psi \triangleq \frac{\tau + \epsilon\delta}{\Xi}$ . Since  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are not adjacent,  $(\phi, \psi) \in \mathcal{Q}_q$  by (ii) of  $\mathcal{Q}$ -criterion 2. Note that it is possible that  $\gcd(\phi, \psi) > 1$ , in which case we can reduce  $(\phi, \psi)$  further to  $(\gamma', \delta') \triangleq (\frac{\phi}{\gcd(\phi, \psi)}, \frac{\psi}{\gcd(\phi, \psi)}) \in \mathcal{Q}_q^{char}$ .

Consider an arbitrary  $\eta \in \mathcal{V}(\frac{\kappa}{\tau})$ . We have

$$\begin{aligned} |\delta'\eta - \gamma'| &\leq |\psi\eta - \phi| = \frac{|(\tau\eta - \kappa) + \epsilon(\delta\eta - \gamma)|}{|\Xi|} \\ &\leq \frac{|\tau\eta - \kappa| + |\delta\eta - \gamma|}{|\Xi|} \\ &\leq \frac{2}{|\Xi|} \max\{|\tau\eta - \kappa|, |\delta\eta - \gamma|\} < |\delta\eta - \gamma|. \end{aligned} \quad (93)$$

where the last inequality holds since  $|\tau\eta - \kappa| \leq |\delta\eta - \gamma|$  for  $\forall \eta \in \mathcal{V}(\frac{\kappa}{\tau})$  and  $|\Xi| = \sqrt{5} > 2$ .

Furthermore, we have

$$\begin{aligned} |\Xi'| &\triangleq |\kappa\delta' - \tau\gamma'| \leq |\kappa\psi - \tau\phi| \leq \frac{|\kappa(\tau + \epsilon\delta) - \tau(\kappa + \epsilon\gamma)|}{|\Xi|} \\ &= \frac{|\kappa\delta - \tau\gamma|}{|\Xi|} = 1 < |\Xi| = \sqrt{5}. \end{aligned} \quad (94)$$

**Lemma 14:** Consider two non-adjacent pairs  $(\kappa, \tau), (\gamma, \delta) \in \mathcal{Q}_q^{char}$  with normalized distance  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| = 1$  or  $\sqrt{2}$ . There exists another pair  $(\gamma', \delta') \in \mathcal{Q}_q^{char}$  such that  $|\delta'\eta - \gamma'| < |\delta\eta - \gamma|, \forall \eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}$  and  $|\delta'\eta - \gamma'| \leq |\delta\eta - \gamma|$  at  $\eta = \frac{\kappa}{\tau}$ . Furthermore,  $|\Xi'| \triangleq |\kappa\delta' - \tau\gamma'| \leq |\Xi| = 1$  or  $\sqrt{2}$ .

*Proof of Lemma 14:* According to  $\mathcal{Q}$ -criterion 1,  $(\phi, \psi) \triangleq (\kappa + \epsilon\gamma, \tau + \epsilon\delta) \in \mathcal{Q}_q$  for  $\forall \epsilon \in \{\pm 1, \pm i\}$ , since  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are not adjacent. Note that it is possible that  $\gcd(\phi, \psi) > 1$ , in which case we can reduce  $(\phi, \psi)$  further to  $(\gamma', \delta') \triangleq \frac{1}{\gcd(\phi, \psi)}(\phi, \psi) \in \mathcal{Q}_q^{char}$ .

Consider an arbitrary  $\eta \in \mathcal{V}(\frac{\kappa}{\tau})$ . Given  $|\tau\eta - \kappa| \leq |\delta\eta - \gamma|$ , we can choose a proper  $\epsilon \in \{\pm 1, \pm i\}$  such that (we can think of  $\tau\eta - \kappa$  and  $\delta\eta - \gamma$  in (95) below as two 2-dimensional vectors on the complex plane and that  $\epsilon = i, -1$ , and  $-i$  rotate  $\delta\eta - \gamma$  by  $\frac{\pi}{2}, \pi$ , and  $\frac{3\pi}{2}$  respectively):

$$\begin{aligned} |\delta'\eta - \gamma'| &\leq |\psi\eta - \phi| = |(\tau\eta - \kappa) + \epsilon(\delta\eta - \gamma)| \\ &\leq |\delta\eta - \gamma|, \end{aligned} \quad (95)$$

where the last inequality in (95) is satisfied with equality only at  $\eta = \frac{\kappa}{\tau}$ . Thus,

$$|\delta'\eta - \gamma'| < |\delta\eta - \gamma|, \forall \eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}, \quad (96)$$

$$\text{and } |\delta'\eta - \gamma'| \leq |\delta\eta - \gamma|, \eta = \frac{\kappa}{\tau}. \quad (97)$$

Furthermore, similar to (94), we can also verify that

$$|\Xi'| \triangleq |\kappa\delta' - \tau\gamma'| \leq |\Xi| = 1 \text{ or } \sqrt{2}. \quad (98)$$

**Remark 10:** The inequality in (97) may be satisfied with equality at  $\eta = \frac{\kappa}{\tau}$ . Thus, potentially, a non-adjacent element can still be a  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference at the “singular point”  $\eta = \frac{\kappa}{\tau}$ . Note, however, this is the only point at which a non-adjacent element can potentially be a  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference. Furthermore, we will argue that there is always an adjacent element that is a  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference at  $\eta = \frac{\kappa}{\tau}$  (see Corollary 1 below). Thus, we can eliminate non-adjacent elements from consideration when we try to identify the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  within the Voronoi region  $\mathcal{V}(\frac{\kappa}{\tau})$ .

**Corollary 1 (T4-2):** Consider two non-adjacent pairs  $(\kappa, \tau) \in \mathcal{Q}_q^{char}$  and  $(\gamma, \delta) \in \mathcal{Q}_q^{char}$ . There exists another pair  $(\gamma', \delta') \in \mathcal{Q}_q^{char}$  adjacent to  $(\kappa, \tau)$  such that  $|\delta'\eta - \gamma'| < |\delta\eta - \gamma|, \forall \eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}$  and  $|\delta'\eta - \gamma'| \leq |\delta\eta - \gamma|$  at  $\eta = \frac{\kappa}{\tau}$ .

*Proof of Corollary 1:* Starting with  $(\gamma, \delta)$  that is non-adjacent to  $(\kappa, \tau)$ , we can apply the results of Lemmas 12, 13, and 14 iteratively to eventually find a pair  $(\gamma', \delta') \in \mathcal{Q}_q^{char}$  that satisfies one of the following:

- (i)  $|\Xi| \triangleq |\kappa\delta' - \tau\gamma'| = 1, \sqrt{2}$  or  $\sqrt{5}$  and that  $(\gamma', \delta')$  is adjacent to  $(\kappa, \tau)$ . We further have that  $|\delta'\eta - \gamma'| < |\delta\eta - \gamma|$  for  $\forall \eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}$ , and that  $|\delta'\eta - \gamma'| \leq |\delta\eta - \gamma|$  at  $\eta = \frac{\kappa}{\tau}$ .
- (ii)  $|\Xi| \triangleq |\kappa\delta - \tau\gamma| = 1$  or  $\sqrt{2}$  but  $(\gamma', \delta')$  is not adjacent to  $(\kappa, \tau)$ . That is, we stop at *Lemma 14* with  $(\gamma', \delta')$  still not adjacent to  $(\kappa, \tau)$ . Note, however, that for *Lemma 14*, we also have  $|\delta'\eta - \gamma'| < |\delta\eta - \gamma|$  for  $\forall \eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}$ , and that  $|\delta'\eta - \gamma'| \leq |\delta\eta - \gamma|$  at  $\eta = \frac{\kappa}{\tau}$ . In this case, we apply *Lemma 14* again to find another pair  $(\gamma'', \delta'')$  with  $|\delta''\eta - \gamma''| < |\delta'\eta - \gamma'|$ ,  $\forall \eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}$ , and that  $|\delta''\eta - \gamma''| \leq |\delta'\eta - \gamma'|$  for  $\eta = \frac{\kappa}{\tau}$ . If this  $(\gamma'', \delta'')$  is still not adjacent to  $(\kappa, \tau)$ , we apply *Lemma 14* yet again to find another pair  $(\gamma''', \delta''')$ . Note that with each successively pair, the weighted distance of the new pair to  $\eta \in \mathcal{V}(\frac{\kappa}{\tau}) \setminus \{\frac{\kappa}{\tau}\}$  becomes strictly smaller than that of the previous pair. Therefore, the successive pairs are distinct and we will never repeat the same pair in the above iterative argument. Since all these pairs are elements of  $\mathcal{Q}_q^{char}$ , and  $\mathcal{Q}_q^{char}$  is a finite set, we must eventually reach a pair that is adjacent to  $(\kappa, \tau)$ . Otherwise, we would be able to enumerate an infinite number of non-adjacent pairs within  $\mathcal{Q}_q^{char}$ .

Now that we have proved (T4-1) and (T4-2), we can narrow our interest to adjacent elements when we try to identify the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining differences within the weighted Voronoi region.

As an illustration, we revisit the Voronoi diagram for  $q = 3$  in Fig. 9 to explore the implications of *Q-criteria 1-3* and *Theorem 4*. We consider a zero- $l_{\min}$  channel gain  $\eta^o = \frac{1+i}{2}$  associated with the characteristic difference  $(\delta_A^{char}, \delta_B^{char}) = (1+i, -i)$ . From Fig. 9, the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining differences for  $\eta$  in  $\mathcal{V}(\eta^o)$  are adjacent to  $(\delta_A^{char}, \delta_B^{char})$ . Some examples of  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining differences are  $(\delta_A^{char'}, \delta_B^{char'}) = \{(2+2i, -i), (2+2i, -1-2i)\}$  with  $|\delta_B^{char} \delta_A^{char'} - \delta_A^{char} \delta_B^{char'}| = \sqrt{2}$  and  $(\delta_A^{char'}, \delta_B^{char'}) \in \{(1+2i, -i), (2+2i, -1-i), (1+2i, -2i), (2+i, -1-2i)\}$  with  $|\delta_B^{char} \delta_A^{char'} - \delta_A^{char} \delta_B^{char'}| = 1$ . We can check that these  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining differences are consistent with our *Q-criteria 1-3*.

Next, we show that a non-adjacent characteristic difference can be a  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference at a particular zero- $l_{\min}$  channel gain, as stated in *Remark 10*. For  $q = 3$ , we consider  $\eta^o = 1$  associated with  $(\delta_A^{char}, \delta_B^{char}) = (1, -1)$ . Further consider  $(\delta_A^{char'}, \delta_B^{char'}) = (1, -1-i)$  associated with  $\eta^{o'} = 1+i$ . We can verify that  $|\delta_B^{char} \delta_A^{char'} - \delta_A^{char} \delta_B^{char'}| = 1$ . However, we can also verify that  $(\delta_A^{char'}, \delta_B^{char'})$  is not adjacent to  $(\delta_A^{char}, \delta_B^{char})$  according to *Q-criterion 1*, since the four medians between  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  are all in the  $\mathcal{Q}_q^{char}$ -set. Therefore, by *Corollary 1*,  $(\delta_A^{char'}, \delta_B^{char'})$  is not the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference within  $\mathcal{V}(-\frac{\delta_B^{char}}{\delta_A^{char}})$  except at  $\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$ . As implied by the proof of *Theorem 2*, any characteristic difference whose normalized distance with  $(\delta_A^{char}, \delta_B^{char})$  is 1 is a  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference at

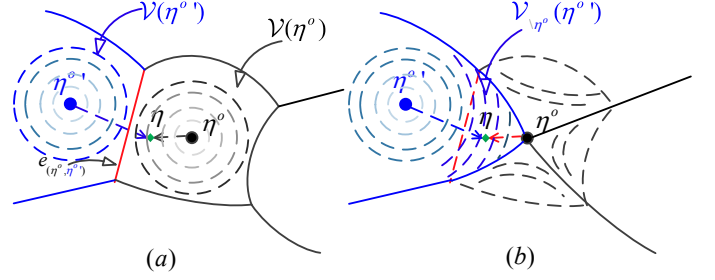


Fig. 11. Weighted Voronoi regions of  $\eta^{o'}$  (a) with consideration of  $\eta^o$  and (b) without consideration of  $\eta^o$  (ROCD). The arc denotes the contour line of a generator.

$\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$ . This characteristic difference has weighted distance of  $\frac{1}{|\delta_A^{char}|}$  (i.e.,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})} = \frac{1}{|\delta_A^{char}|}$  at  $\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$ ). Since the normalized distance of  $(\delta_A^{char'}, \delta_B^{char'})$  and  $(\delta_A^{char}, \delta_B^{char})$  is 1,  $(\delta_A^{char'}, \delta_B^{char'})$  is  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference at  $\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$ . However, the adjacent difference  $(\delta_A^{char''}, \delta_B^{char''}) = (2, -2-i)$  is also the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference at  $\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$ , since its normalized distance with  $(\delta_A^{char}, \delta_B^{char})$  is also 1. Thus, when deriving the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ -determining difference within  $\mathcal{V}(-\frac{\delta_B^{char}}{\delta_A^{char}})$ , we need not consider  $(\delta_A^{char'}, \delta_B^{char'})$ .

#### G. Overview of $l_{\min}$ and $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$

With reference to Fig. 9, we now illustrate how  $l_{\min}$  and  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  change as the channel gain varies. Consider two characteristic differences  $(\delta_A^{char}, \delta_B^{char})$  and  $(\delta_A^{char'}, \delta_B^{char'})$  associated with  $\eta^o$  and  $\eta^{o'}$  that are adjacent to each other. For simplicity, we denote the “new” weighted Voronoi region of an element  $(\delta_A^{char'}, \delta_B^{char'})$  after we remove  $(\delta_A^{char}, \delta_B^{char})$  as  $\mathcal{V} \setminus \{-\frac{\delta_B^{char}}{\delta_A^{char}}\} (-\frac{\delta_B^{char'}}{\delta_A^{char'}})$  by ROCD.

Consider  $l_{\min}$  shown in Fig. 11(a). In this region,  $l_{\min}$  reaches the minimum at  $\eta^o$  (the vertex of the cone). Then,  $l_{\min}$  increases as  $\eta$  approaches the edges of  $\mathcal{V}(-\frac{\delta_B^{char}}{\delta_A^{char}})$  and reaches a local maximum at an edge of this Voronoi region (the intersections of two cones). When  $\eta$  crosses the edges and falls into  $\mathcal{V}(-\frac{\delta_B^{char'}}{\delta_A^{char'}})$ ,  $(\delta_A^{char'}, \delta_B^{char'})$  will yield  $l_{\min}$ , but the variation of  $l_{\min}$  in this Voronoi region still follows the same pattern as above. As long as  $\eta$  is within the same weighted Voronoi region,  $l_{\min}$  varies in a continuous fashion following the contour as expressed in (28).

Consider  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  in  $\mathcal{V}(-\frac{\delta_B^{char}}{\delta_A^{char}})$  shown in Fig. 11(b). We show how a subset of the region  $\mathcal{V}(-\frac{\delta_B^{char}}{\delta_A^{char}})$  becomes part of  $\mathcal{V} \setminus \{-\frac{\delta_B^{char}}{\delta_A^{char}}\} (-\frac{\delta_B^{char'}}{\delta_A^{char'}})$  after ROCD (i.e.,  $(\delta_A^{char'}, \delta_B^{char'})$  yields  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  within a subset of the region of  $\mathcal{V}(-\frac{\delta_B^{char}}{\delta_A^{char}})$ ). First,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  reaches a local maximum at  $\eta^o = -\frac{\delta_B^{char}}{\delta_A^{char}}$ , since we observe that all adjacent elements of  $\eta^o$ , separated with  $(\delta_A^{char}, \delta_B^{char})$  by a normalized distance of 1, meet at  $\eta^o$



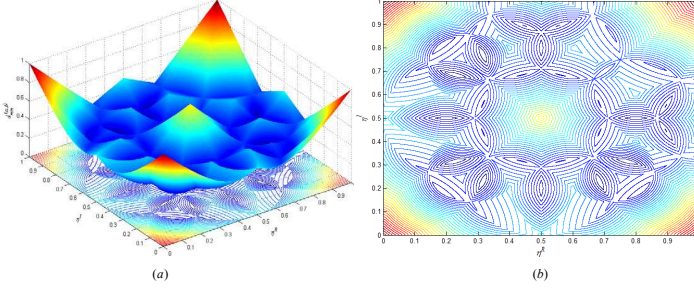


Fig. 12. (a)  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}(\eta)$  surface for  $q = 3$  and  $|\eta| \leq 2$ ; (b) the corresponding contour graphs of  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}(\eta)$ .

after ROCD. Then, within  $\mathcal{V} \setminus \{-\frac{\delta_B^{char}}{\delta_A^{char}}\}(-\frac{\delta_B^{char'}}{\delta_A^{char'}})$ , we observe that  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  decreases as  $\eta$  approaches the edge of  $\eta^o$  and  $\eta^{o'}$  (see contour lines of  $\eta^{o'}$  after ROCD in Fig. 11(b)), and reaches a local minimum at the edge, i.e.,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})} = l_{\min}$ . Furthermore, when  $\eta$  crosses the edge and falls into  $\mathcal{V}(-\frac{\delta_B^{char'}}{\delta_A^{char'}})$ ,  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  will be determined by a different characteristic difference, but still follows the same pattern as above. In general, the local minima of  $l_{\min}$  correspond to local maxima of  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  and the local maxima of  $l_{\min}$  correspond to the local minima of  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  in the overall complex plane of  $\eta$ .

As an illustrating example, we plot the  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  versus  $\eta$  for  $q = 3$  in Fig. 12. With respect to the  $l_{\min}$  versus  $\eta$  plot in Fig. 5, we can observe that the changes of  $l_{\min}$  and  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$  are consistent with our analysis above.

## VII. CONCLUSION

We have investigated a general framework of complex linear PNC for TWRC, where the signals of the two end nodes simultaneously received at the relay incur imbalanced powers and a relative phase offset. Specifically, we put forth a Gaussian-integer formulation for the complex linear PNC mapping in  $\mathbb{Z}[i]/q$ . Our Gaussian-integer formulation provides more flexibility for signal constellation designs than the vector formulation in prior work. We further recast the linear PNC mapping based on the coset theory to uncover the isomorphism among PNC mappings. The isomorphism allows us to reduce the search space for the optimal PNC mapping by selecting one representative PNC mapping from each isomorphic group.

For each channel gain ratio  $\eta = h_A/h_B$ , there is a corresponding optimal PNC mapping  $(\alpha_{opt}, \beta_{opt})$ . To identify  $(\alpha_{opt}, \beta_{opt})$  for a given  $\eta$ , we focused on the characterization of two minimum-distance metrics in the received constellation. The first minimum-distance metric is the minimum *symbol* distance  $l_{\min}$ , which is the minimum distance among all distances between two constellation points. The second minimum-distance metric is the minimum *NC-symbol* distance  $d_{\min}^{(\alpha, \beta)}$  under PNC mapping  $(\alpha, \beta)$ , which is the minimum distance among all distances between two constellation points mapped to different NC symbols by  $(\alpha, \beta)$ . It is  $d_{\min}^{(\alpha, \beta)}$  that determines the SER of NC symbols in the high SNR regime. The optimal PNC mapping is given by  $(\alpha_{opt}, \beta_{opt}) = \arg \max_{(\alpha, \beta)} d_{\min}^{(\alpha, \beta)}$ .

An important concept put forth in this paper is the *characteristic difference*  $(\delta_A^{char}, \delta_B^{char}) = (w_A, w_B) - (w'_A, w'_B)$ : the difference between any two distinct joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  for which there is no common factor between  $\delta_A^{char}$  and  $\delta_B^{char}$  (i.e.,  $\gcd(\delta_A^{char}, \delta_B^{char}) = \text{unit}$ ). Given a set of joint symbols  $\mathcal{W}_{(A, B)} = \{(w_A, w_B) | w_A, w_B \in \mathbb{Z}[i]/q\}$ , there is a corresponding set of characteristic differences. For a given  $\eta$ ,  $l_{\min}$  is given by the particular characteristic difference that yields the minimum  $|\eta \delta_A^{char} + \delta_B^{char}|$ . The optimal PNC mapping  $(\alpha_{opt}, \beta_{opt})$  for that  $\eta$  is the mapping that maps two pairs of symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  separated by  $(\delta_A^{char}, \delta_B^{char})$  to the same NC symbol, hence there is no need to distinguish between  $(w_A, w_B)$  and  $(w'_A, w'_B)$  although the distance between them in the received constellation is  $l_{\min}$ .

For a global understanding of how  $l_{\min}$  and  $d_{\min}^{(\alpha, \beta)}$  vary with  $\eta$ , we investigated the partitioning of the complex plane of  $\eta$  into different Voronoi regions. The  $\eta$  within a Voronoi region are associated with the same characteristic difference  $(\delta_A^{char}, \delta_B^{char})$  and the same optimal PNC mapping  $(\alpha_{opt}, \beta_{opt})$  (i.e.,  $(\delta_A^{char}, \delta_B^{char})$  induces the  $l_{\min} = |\eta \delta_A^{char} + \delta_B^{char}|$ , and  $(\alpha_{opt}, \beta_{opt})$  maps joint symbols separated by  $(\delta_A^{char}, \delta_B^{char})$  to the same NC symbol). We developed a systematic approach to identify the  $d_{\min}^{(\alpha, \beta)}$  for all  $\eta$  within a Voronoi region by considering the characteristic differences associated with Voronoi regions adjacent to it.

As a final remark, we believe that our framework of complex linear PNC mapping in the field of Gaussian integer—including the concept of characteristic difference, isomorphism via coset theory, Voronoi-region characterization of optimal PNC mapping, and determination of  $d_{\min}^{(\alpha_{opt}, \beta_{opt})}$ —is also applicable to complex linear PNC mappings in other fields (e.g., the finite field of Eisenstein integer), since the underlying mathematical concepts are similar.

## APPENDIX I: ALGEBRAIC CONSTRUCTION OF VALID NC MAPPING

Consider an NC mapping under  $(\alpha, \beta)$  in (5). *Propositions 6 and 7* below specify how the set of joint symbols are partitioned by this NC mapping and show the isomorphism in NC mappings in terms of cosets in group theory.

With respect to  $\Delta_{(\alpha, \beta)}$  in (13), we define a corresponding set within the finite field of  $\mathbb{Z}[i]/q$  as follows:

$$\Delta_{(\alpha, \beta)}^{(q)} = \{(\delta_A^{(q)}, \delta_B^{(q)}) = (\delta_A \pmod{q}, \delta_B \pmod{q}) | (\delta_A, \delta_B) \in \Delta_{(\alpha, \beta)}\}. \quad (99)$$

Given a  $(\delta_A, \delta_B) \in \Delta_{(\alpha, \beta)}$  and its corresponding  $(\delta_A^{(q)}, \delta_B^{(q)}) = (\delta_A \pmod{q}, \delta_B \pmod{q}) \in \Delta_{(\alpha, \beta)}^{(q)}$ , we use the terms “the NC mapping  $(\alpha, \beta)$  clusters  $(\delta_A, \delta_B)$ ” and “the NC mapping  $(\alpha, \beta)$  clusters  $(\delta_A^{(q)}, \delta_B^{(q)})$ ” interchangeably in this appendix.

It is easy to show that  $\Delta_{(\alpha, \beta)}^{(q)}$  is a group under element-wise addition operation of  $\mathbb{Z}^2[i]/q$ , where  $\Delta_{(\alpha, \beta)}^{(q)} = \Delta_{(\alpha, \beta)} \pmod{q}$ . Closure and associativity are obvious. The identity element of the group is simply  $e \triangleq (0, 0) \pmod{q}$ , and the inverse of an element  $\delta \triangleq (\delta_A^{(q)}, \delta_B^{(q)}) \in \mathbb{Z}^2[i]/q$  is simply  $-\delta \triangleq (-\delta_A^{(q)}, -\delta_B^{(q)}) \pmod{q}$ .

Let us see how to enumerate the elements in  $\Delta_{(\alpha,\beta)}^{(q)}$ . We first note that  $(\delta_A^{(q)'}, \delta_B^{(q)'}) = (-\beta, \alpha)$  is a solution to (13). We next note that (13) can be satisfied by  $(\delta_A^{(q)}, \delta_B^{(q)}) = v(\delta_A^{(q)'}, \delta_B^{(q)'}) \pmod{q}$ ,  $\forall v \in \mathbb{Z}[i]/q$ . Thus, there are altogether  $|q|^2$   $(\delta_A^{(q)}, \delta_B^{(q)})$  that can satisfy (13). Therefore,  $\Delta_{(\alpha,\beta)}^{(q)}$  can be rewritten as

$$\Delta_{(\alpha,\beta)}^{(q)} = \{(\delta_A^{(q)}, \delta_B^{(q)}) \in (\mathbb{Z}[i]/q)^2 \mid (\delta_A^{(q)}, \delta_B^{(q)}) = v(-\beta, \alpha) \pmod{q}\}. \quad (100)$$

Thus, under  $(\alpha, \beta)$ , two joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  will be mapped to the same NC symbol if and only if

$$(w_A, w_B) = (w'_A, w'_B) + v(-\beta, \alpha) \pmod{q} \quad (101)$$

for some  $v \in \mathbb{Z}[i]/q$ . Note that, for simplicity, we include the trivial case  $v = 0$  where  $(w_A, w_B)$  and  $(w'_A, w'_B)$  are the same symbol.

**Definition 14 (Coset):** In algebra, if  $G$  is a group with operation  $\circ$ ,  $H$  is a subgroup of  $G$  and  $g \in G$ , then

$g \circ H = \{g \circ h \mid h \in H\}$  is a left coset of  $H$  in  $G$ , and  $H \circ g = \{h \circ g \mid h \in H\}$  is a right coset of  $H$  in  $G$ .

For abelian groups, the left and right cosets are the same [20].

For us,  $G$  is the additive group of  $\mathbb{Z}^2[i]/q$  (i.e., the group is  $(\mathbb{Z}^2[i]/q, +)$  where  $+$  is the element-wise addition). The collection of all joint symbols is the set  $\mathcal{W}_{(A,B)} = \mathbb{Z}^2[i]/q$ . For a given NC mapping  $(\alpha, \beta)$ , a subgroup of  $G$  is  $H \triangleq \Delta_{(\alpha,\beta)}^{(q)}$ .

Consider a joint symbol  $(w_A, w_B) \in \mathbb{Z}^2[i]/q$ . The coset  $(w_A, w_B) + \Delta_{(\alpha,\beta)}^{(q)} \pmod{q}$  is the set of all joint symbols mapped to the same NC symbol as  $(w_A, w_B)$ . That is, a coset consists of all joint symbols mapped to the same NC symbol. Given any element of a coset, i.e.,  $(w_A, w_B)$ , we can find all elements of the coset by  $(w_A, w_B) + \Delta_{(\alpha,\beta)}^{(q)} \pmod{q}$  if we know  $\Delta_{(\alpha,\beta)}^{(q)}$ . The elements in  $\Delta_{(\alpha,\beta)}^{(q)}$  can be found from (100).

The following proposition summarizes the discussion above.

**Proposition 6:** A linear NC mapping under  $(\alpha, \beta)$  partitions the set of joint symbols  $\mathcal{W}_{(A,B)} = \mathbb{Z}^2[i]/q$  into  $|q|^2$  subsets, each mapped to a unique NC symbol. Consider the additive group of  $\mathcal{W}_{(A,B)}$ . Each of the  $|q|^2$  subset is a coset generated by the subgroup  $\Delta_{(\alpha,\beta)}^{(q)}$  of  $\mathcal{W}_{(A,B)}$ , described as follows:

$$\Delta_{(\alpha,\beta)}^{(q)} = \{(\delta_A^{(q)}, \delta_B^{(q)}) \in \mathbb{Z}^2[i]/q \mid \alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}\}. \quad (102)$$

The subgroup  $\Delta_{(\alpha,\beta)}^{(q)}$  contains  $|q|^2$  elements and they can be found as follows:

$$\Delta_{(\alpha,\beta)}^{(q)} = \{(\delta_A^{(q)}, \delta_B^{(q)}) \in \mathbb{Z}^2[i]/q \mid (\delta_A^{(q)}, \delta_B^{(q)}) = v(-\beta, \alpha) \pmod{q}, v \in \mathbb{Z}[i]/q\}. \quad (103)$$

For a joint symbol  $(w_A, w_B) \in \mathbb{Z}^2[i]/q$ ,

$$\mathcal{C}_w = \{(w'_A, w'_B) \mid (w'_A, w'_B) = (w_A, w_B) + (\delta_A^{(q)}, \delta_B^{(q)}) \pmod{q}, (\delta_A^{(q)}, \delta_B^{(q)}) \in \Delta_{(\alpha,\beta)}^{(q)}\}. \quad (104)$$

is a coset of  $\Delta_{(\alpha,\beta)}^{(q)}$  in  $\mathbb{Z}^2[i]/q$ . Each coset contains  $|q|^2$  distinct joint symbols. ■

From *Proposition 6*, the complex NC mapping  $f_N^{(\alpha,\beta)} : \mathcal{W}_{(A,B)} \rightarrow \mathcal{W}_N^{(\alpha,\beta)}$  is a  $|q|^2$ -to-1 mapping. This NC mapping partitions  $\mathcal{W}_{(A,B)}$  into  $|q|^2$  subsets (i.e.,  $|q|^2$  cosets). We say that these  $|q|^2$  cosets are *generated* by  $(\alpha, \beta)$ . Each of these cosets is *labeled* by an NC symbol to which the elements within the coset is mapped. To find the NC symbol that serves as the label, we simply take an element  $(w_A, w_B)$  from the coset, and then compute  $\alpha w_A + \beta w_B \pmod{q}$ .

**Proposition 7:** The cosets generated by  $\Delta_{(\alpha,\beta)}^{(q)}$  are the same as the cosets generated by  $\Delta_{(\gamma\alpha, \gamma\beta)}^{(q)} \pmod{q}$  where  $\gamma \in \mathbb{Z}[i]/q \setminus \{0\}$ .

**Proof of Proposition 7:** Consider an arbitrary element  $(\delta_A^{(q)}, \delta_B^{(q)}) \in \Delta_{(\alpha,\beta)}^{(q)}$ . Then, we have  $\alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}$ . For  $\gamma \in \mathbb{Z}[i]/q \setminus \{0\}$ , we further have

$$\gamma(\alpha\delta_A^{(q)} + \beta\delta_B^{(q)}) = (\gamma\alpha)\delta_A^{(q)} + (\gamma\beta)\delta_B^{(q)} = 0 \pmod{q}. \quad (105)$$

Thus,  $(\delta_A^{(q)}, \delta_B^{(q)}) \in \Delta_{(\gamma\alpha, \gamma\beta)}^{(q)} \pmod{q}$ .

Similarly, consider an arbitrary element  $(\delta_A^{(q)}, \delta_B^{(q)}) \in \Delta_{(\gamma\alpha, \gamma\beta)}^{(q)} \pmod{q}$ . Then,  $(\gamma\alpha)\delta_A^{(q)} + (\gamma\beta)\delta_B^{(q)} = 0 \pmod{q}$ . Since  $\gamma \in \mathbb{Z}[i]/q \setminus \{0\}$ , we further have  $\gamma^{-1}((\gamma\alpha)\delta_A^{(q)} + (\gamma\beta)\delta_B^{(q)}) = \alpha\delta_A^{(q)} + \beta\delta_B^{(q)} = 0 \pmod{q}$ , where  $\gamma^{-1}$  is the multiplicative inverse of  $\gamma$ . Thus,  $(\delta_A^{(q)}, \delta_B^{(q)}) \in \Delta_{(\alpha,\beta)}^{(q)}$ .

Therefore,  $\Delta_{(\alpha,\beta)}^{(q)} = \Delta_{(\gamma\alpha, \gamma\beta)}^{(q)} \pmod{q}$  and the cosets generated by  $\Delta_{(\alpha,\beta)}^{(q)}$  and  $\Delta_{(\gamma\alpha, \gamma\beta)}^{(q)} \pmod{q}$  are the same. ■

**Remark 11:** The above results mean that the NC partitioning of  $\mathcal{W}_{(A,B)}$  into  $|q|^2$  cosets are the same under  $(\alpha, \beta)$  and  $(\gamma\alpha, \gamma\beta) \pmod{q}$ ,  $\forall \gamma \in \mathbb{Z}[i]/q \setminus \{0\}$ . However, the NC symbols used to label the same coset are different under  $(\alpha, \beta)$  and  $(\gamma\alpha, \gamma\beta)$  when  $\gamma \neq 1$ . Specifically, the NC mappings induced by  $(\alpha, \beta)$  and  $(\gamma\alpha, \gamma\beta) \pmod{q}$  are isomorphic as per *Definition 3*. Note that given  $(\delta_A^{(q)}, \delta_B^{(q)})$ , the NC mapping  $(\alpha, \beta)$  that clusters  $(\delta_A^{(q)}, \delta_B^{(q)})$  is unique except for  $(\gamma\alpha, \gamma\beta) \pmod{q}$ . In this paper, we say that  $(\alpha, \beta)$  clusters  $(\delta_A^{(q)}, \delta_B^{(q)})$  uniquely if any other  $(\alpha', \beta')$  that can also cluster  $(\delta_A^{(q)}, \delta_B^{(q)})$  does not alter the partitioning of  $\mathcal{W}_{(A,B)}$  into  $|q|^2$  cosets. Therefore, the NC mappings under  $(\alpha, \beta)$  and  $(\gamma\alpha, \gamma\beta) \pmod{q}$  yield the same NC partitioning. Note that uniqueness in this sense can be assured for Gaussian prime  $q$  thanks to finite-field arithmetic.

Below is a corollary of *Proposition 7*, which rephrases *Proposition 3* from the coset perspective.

**Corollary 2:** For a specific set of cosets generated by  $(\alpha, \beta)$ , there exists a corresponding  $(\alpha', \beta') = (\beta^{-1}\alpha, 1) \pmod{q}$  generating the same set of cosets.

**Proof of Proposition 2:** Consider a set of cosets generated by  $\Delta_{(\alpha,\beta)}^{(q)}$ . We choose  $\gamma$  to be the multiplicative inverse of  $\beta$ , i.e.,  $\beta\gamma = 1$ . Here,  $\gamma$  exists since  $\beta \in \mathbb{Z}[i]/q \setminus \{0\}$ . By *Proposition 7*,  $\Delta_{(\alpha,\beta)}^{(q)} = \Delta_{(\beta^{-1}\alpha, 1)}^{(q)} \pmod{q}$ . Therefore, the corresponding  $(\alpha', \beta') = (\beta^{-1}\alpha, 1) \pmod{q}$ . ■



## APPENDIX II - PROOF OF LEMMA 2

When  $|q| < \sqrt{5}$  (i.e.,  $|q| = \sqrt{2}$ ), we have  $\mathbb{Z}[i]/q = \{0, 1\}$  by *Remark 1*. Then,  $\delta_A, \delta_B \in \{0, \pm 1\}$  and  $\delta_A$  and  $\delta_B$  cannot be both zero if the  $(\delta_A, \delta_B)$  is a distance-valid difference pair. Therefore,  $|\delta_A|, |\delta_B| \leq 1 \leq \sqrt{2|q|^2 - 4q^R + 2} = \sqrt{2\sqrt{2}^2 - 4 + 2} = \sqrt{2}$ .

In the following, we consider  $|q| \geq \sqrt{5}$ . We consider  $\delta_A$  only and the proof for  $\delta_B$  is similar. The difference between any two distinct representative elements  $w_A$  and  $w'_A$  in  $\mathbb{Z}[i]/q$  is upper-bounded as follows:

$$|\delta_A| = |w_A - w'_A| \leq |w_A| + |w'_A| \leq 2 \max_{w_A \in \mathbb{Z}[i]/q} |w_A|. \quad (106)$$

To derive  $\max |w_A|$  in  $\mathbb{Z}[i]/q$ , let us consider the center of the square formed by  $q$  and  $iq$ , i.e., the point A (see the cross in Fig. 2) and

$$\begin{aligned} A &= \frac{1}{2}(q^R + iq^I) + \frac{1}{2}(-q^I + iq^R) \\ &= \frac{1}{2}(q^R - q^I) + i\frac{1}{2}(q^R + q^I). \end{aligned} \quad (107)$$

Note that point A is a vertex of the square within which all valid symbols lie (i.e., the blue square in Fig. 2; according to *Definition 1*, representative elements lie within the zero-centered square of side length  $|q|$  with orientation aligned with the directions as indicated by the basis  $(x, y)$ —see the red stars within the blue squares in Fig. 2).

Point A is the point with the largest magnitude within the square. However, A is not a valid symbol (i.e.,  $A \notin \mathbb{Z}[i]/q$ ), since it is not a Gaussian integer. Thus,  $|A| > \max_{w_A \in \mathbb{Z}[i]/q} |w_A|$ . We claim that the valid symbol that is closest to A is a symbol with the maximum magnitude.

Specifically, we claim that  $w_A^* \triangleq A - (\frac{1}{2} + i\frac{1}{2}) = \max_{w_A \in \mathbb{Z}[i]/q} |w_A|$ . First, for  $w_A^* = A - (\frac{1}{2} + i\frac{1}{2})$ , we can easily verify that  $w_A^{*x}, w_A^{*y} < \frac{|q|}{2}$  by *Definition 1*, and therefore  $w_A^*$  is a valid symbol. Furthermore,

$$\begin{aligned} |w_A^*| &= \left| \frac{1}{2}(q^R - q^I - 1) + i\frac{1}{2}(q^R + q^I - 1) \right| \\ &= \sqrt{\frac{|q|^2}{2} - q^R + \frac{1}{2}}. \end{aligned} \quad (108)$$

In the following, we prove that  $w_A^* = \arg \max_{w_A \in \mathbb{Z}[i]/q} |w_A|$  by showing that  $|w_A^*| \geq |w_A|, \forall w_A \in \mathbb{Z}[i]/q$ . Given an arbitrary valid symbol  $w_A \in \mathbb{Z}[i]/q$ , we can verify that three other Gaussian integers, i.e.,  $\{-w_A, iw_A, -iw_A\}$ , are also valid symbols in  $\mathbb{Z}[i]/q$ , symmetric to  $w_A$  with respect to four quadrants in the complex plane. By this symmetry property, we focus on the complex quadrant (angle from 0 to  $\pi/2$ ) in which A lies.

Consider a real Gaussian prime  $q$  (i.e.,  $q^R \neq 0$  and  $q^I = 0$ ). W.l.o.g., suppose that  $q > 0$ . The representative elements of  $\mathbb{Z}[i]/q$  by *Definition 1* are shown in Fig. 2(b). In this case, the point A is  $A = \frac{1}{2}(q + iq)$ , and we can see that  $w_A^* = A - (\frac{1}{2} + i\frac{1}{2})$  is a valid symbol in  $\mathbb{Z}[i]/q$  and  $w_A^* = \arg \max_{w_A \in \mathbb{Z}[i]/q} |w_A|$ . Then, we have  $|\delta_A| \leq 2|A - (\frac{1}{2} + i\frac{1}{2})| = 2|\frac{1}{2}(q - 1) + i\frac{1}{2}(q - 1)| = \sqrt{2}(q - 1)$ . Therefore, we have proved *Lemma 3* when  $q = q^R$ .

Consider a complex Gaussian prime  $q$ , where  $|q| \geq \sqrt{5}$  and  $q^R \neq 0, q^I \neq 0$ . W.l.o.g., we assume  $q^R > q^I \geq 1$  (note that  $q^R \neq q^I$  because  $q$  is prime). We want to prove that  $w_A^* = A - (\frac{1}{2} + i\frac{1}{2})$  is the largest valid symbol within this quadrant. Consider an arbitrary valid symbol  $w$  in  $\mathbb{Z}[i]/q$  within this quadrant

$$w = A - (a + ib) = \left(\frac{q^R - q^I}{2} - a\right) + i\left(\frac{q^R + q^I}{2} - b\right), \quad (109)$$

$$\begin{aligned} |w|^2 &= \left(\frac{q^R - q^I}{2} - a\right)^2 + \left(\frac{q^R + q^I}{2} - b\right)^2 \\ &= \frac{|q|^2}{2} + a[a - (q^R - q^I)] + b[b - (q^R + q^I)]. \end{aligned} \quad (110)$$

where

$$\frac{q^R - q^I}{2} - a \in \mathbb{Z}, \frac{q^R + q^I}{2} - b \in \mathbb{Z}, \quad (111a)$$

$$\frac{q^R - q^I}{2} \geq a, \frac{q^R + q^I}{2} \geq b. \quad (111b)$$

From (111a),  $|a| \geq \frac{1}{2}$  if  $w$  in (109) is a Gaussian integer. Since  $w \in \mathbb{Z}[i]/q$ , we have  $|w^x|, |w^y| < \frac{|q|}{2}$  by *Definition 1*, where

$$\begin{aligned} \begin{pmatrix} w^x \\ w^y \end{pmatrix} &= \frac{1}{|q|} \begin{pmatrix} q^R & q^I \\ -q^I & q^R \end{pmatrix} \begin{pmatrix} \frac{q^R - q^I}{2} - a \\ \frac{q^R + q^I}{2} - b \end{pmatrix} \\ &= \begin{pmatrix} \frac{|q|^2 - 2aq^R - 2bq^I}{2|q|} \\ \frac{|q|^2 - 2bq^R + 2aq^I}{2|q|} \end{pmatrix}. \end{aligned} \quad (112)$$

From (112), we further have

$$\begin{aligned} 0 &< aq^R + bq^I < |q|^2, \\ 0 &< bq^R - aq^I < |q|^2. \end{aligned}$$

Given  $|a| \geq 1/2$ , we next prove that  $|w| \leq |w_A^*|, \forall w \in \mathbb{Z}[i]/q$  by considering the following cases.

**Case 1:**  $a \geq 1/2$  and  $b \geq 1/2$

Obviously, from (110),  $|w| \leq |w_A^*|$ .

**Case 2:**  $a \geq 1/2$  and  $b < 1/2$

This case is not possible if  $w$  is to be valid in  $\mathbb{Z}[i]/q$  (see the blue dashed squares in Fig. 2.).

**Case 3:**  $a \leq -1/2$  and  $b \geq 1/2$

From (111a), we let  $a = -\frac{1+2m}{2}$  and  $b = \frac{1+2n}{2}$ , where  $m \geq 0$  and  $n \geq 0$ . Therefore, (110) can be rewritten as

$$\begin{aligned} |w|^2 &= \frac{|q|^2}{2} + a[a - (q^R - q^I)] + b[b - (q^R + q^I)] \\ &= \frac{|q|^2}{2} + m^2 + n^2 + m + n + \frac{1}{2} \\ &\quad - (n - m)q^R - (m + n + 1)q^I. \end{aligned} \quad (114)$$

From (111b) and (113), we have

$$q^R + q^I \geq 1 + 2n, \quad (115a)$$

$$\frac{1 + 2m}{1 + 2n} < \frac{q^I}{q^R}. \quad (115b)$$

From (115b), we have

$$n > m, \quad (116)$$

since  $q^R > q^I$ . Furthermore, from (115), we have

$$q^I > \frac{1+2m}{1+2n}q^R \geq \frac{1+2m}{q^R+q^I}q^R > \frac{1+2m}{2q^R}q^R = \frac{1}{2} + m. \quad (117)$$

To find a valid  $w \in \mathbb{Z}[i]/q$  such that  $|w| > |w_A^*|$ , we need

$$\begin{aligned} & \frac{|q|^2}{2} + m^2 + n^2 + m + n + \frac{1}{2} - (n-m)q^R - (m+n+1)q^I \\ & > \frac{|q|^2}{2} - q^R + \frac{1}{2}, \end{aligned} \quad (118)$$

$$\Rightarrow m^2 + n^2 + m + n$$

$$- (n-m-1)q^R - (m+n+1)q^I > 0. \quad (119)$$

To check whether  $w$  yielding (119) exists, we consider two subcases as follows:

(3-1)  $2q^I > 1 + 2n$

In this subcase, we have  $q^R > q^I > \frac{1}{2} + n$ . Then, LHS of (119) can be upper bounded as

$$\begin{aligned} & m^2 + n^2 + m + n - (n-m-1)q^R - (n+m+1)q^I \\ & < m^2 + n^2 + m + n - (n-m-1)\left(\frac{1}{2} + n\right) \\ & \quad - (n+m+1)\left(\frac{1}{2} + n\right) \\ & = m^2 + n^2 + m + n - 2n\left(\frac{1}{2} + n\right) \\ & = (m+n)(m-n) + m < 0, \end{aligned} \quad (120)$$

where the first inequality holds since  $q^R > q^I > \frac{1}{2} + n$ , and the last inequality holds since  $n > m$  because of (116). This contradicts with (118). Therefore, in this subcase,  $w^*$  has the largest magnitude among the valid symbols in  $\mathbb{Z}[i]/q$ .

(3-2)  $2q^I < 1 + 2n$

Since  $q^I < \frac{1}{2} + n$  and  $q^I$  is an integer, we have  $q^I \leq n$ . From (115a), we further have  $q^R > 1 + n$ , since  $q^R + n \geq q^R + q^I > 1 + 2n$ .

Then, LHS of (118) can be upper bounded as

$$\begin{aligned} & m^2 + n^2 + m + n - (n-m-1)q^R - (n+m+1)q^I \\ & = m^2 + n^2 - (n-m-1)q^R - (n+m+1)(q^I - 1) - 1 \\ & < m^2 + n^2 - (n-m-1)(n+1) \\ & \quad - (m+n+1)(q^I - 1) - 1 \\ & = m^2 + mn + m - (m+n+1)(q^I - 1) \\ & = (m+n+1)(m - q^I + 1) \leq 0, \end{aligned} \quad (121)$$

where the first inequality holds since  $q^R > 1 + n$ , and the last inequality holds since  $m+1 \leq q^I$  in (117). Therefore, in this subcase,  $w^*$  has the largest magnitude among the valid symbols in  $\mathbb{Z}[i]/q$ .

**Case 4:**  $a \leq -\frac{1}{2}$  and  $b < \frac{1}{2}$

This case is not possible if  $w$  is to be valid in  $\mathbb{Z}[i]/q$ .

### APPENDIX III - PROOF OF LEMMA 3

We need to show that we can find two valid joint symbols  $(w_A, w_B)$  and  $(w'_A, w'_B)$  (i.e.,  $w_A, w_B, w'_A, w'_B$  such that  $w_A - w'_A = \delta_A$  and  $w_B - w'_B = \delta_B$  in the statement of the lemma. In the following, we show that we can find  $w_A$

and  $w'_A$  such that  $w_A - w'_A = \delta_A$  (similar proof applies for  $\delta_B$ ).

When  $|q| < \sqrt{5}$  (i.e.,  $|q| = \sqrt{2}$ ), we have  $\mathbb{Z}[i]/q = \{0, 1\}$  by Remark 1. Therefore, if  $|\delta_A| < |q| = \sqrt{2}$  and  $|\delta_A| \neq 0$ , we must have  $|\delta_A| = 1$  (since  $\delta_A$  is a Gaussian integer). We can choose  $w_A = \delta_A$  and  $w'_A = 0$ .

We next consider  $|q| \geq \sqrt{5}$ . Fig. 13 gives the roadmap of the lengthy proof. First, P1 below gives the proof for the case of  $q^R = 0$  or  $q^I = 0$  (thus, this includes the case of real  $q$ ). Then, P2 proves the case of  $q^R \neq 0$  or  $q^I \neq 0$ , assuming  $q^R > q^I \geq 1$ , focusing on  $\delta_A = q^R + i(q^I - 1)$  (this is the  $\delta_A$  with the largest magnitude that yields  $|\delta_A| < |q|$ ). After that, P3-P5 prove the cases of  $\delta_A$  with  $|\delta_A| < |q^R + i(q^I - 1)|$ .

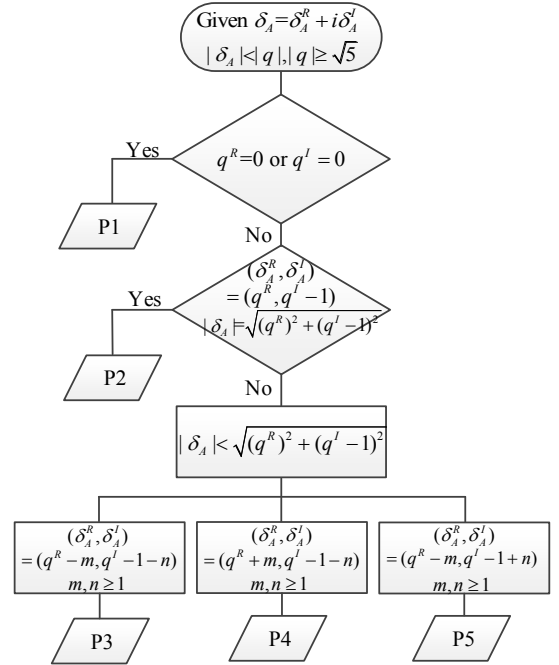


Fig. 13. The proof sketch of Lemma 3.

**P1)** We first consider the case when  $q$  is a real integer prime (i.e.,  $q^I = 0$ ). The proof of the case when  $q^R = 0$  is similar. Since  $q$  is real, we have  $q = |q|$ . Furthermore, we verify that  $w_A^R = w_A^x, w_A^I = w_A^y$  by Definition 1. If  $|\delta_A| = |\delta_A^R + i\delta_A^I|$  and  $q$  is real, we have  $|\delta_A^R|, |\delta_A^I| \leq q - 1$ . Then, we consider the following cases:

P1-1)  $\delta_A^R$  is even,  $\delta_A^I$  is even

In this case, we choose  $w_A = \frac{\delta_A^R}{2} + i\frac{\delta_A^I}{2}$  and  $w'_A = -\frac{\delta_A^R}{2} - i\frac{\delta_A^I}{2}$ . Therefore, by Definition 1,  $w_A, w'_A \in \mathbb{Z}[i]/q$  since  $w_A^R, w_A^I, w_A'^R, w_A'^I < q/2$ .

P1-2)  $\delta_A^R$  is odd,  $\delta_A^I$  is odd

In this case, we further have  $\delta_A^R, \delta_A^I \leq q - 2$ , since the integer prime  $q$  is odd and  $\delta_A^R, \delta_A^I \leq q - 1$ . We choose  $w_A = \frac{\delta_A^R - 1}{2} + i\frac{\delta_A^I - 1}{2}$  and  $w'_A = -\frac{\delta_A^R + 1}{2} - i\frac{\delta_A^I + 1}{2}$ . Therefore, by Definition 1,  $w_A, w'_A \in \mathbb{Z}[i]/q$  since  $w_A^R, w_A^I, w_A'^R, w_A'^I < q/2$ .

P1-3)  $\delta_A^R$  is even,  $\delta_A^I$  is odd

In this case, we further have  $\delta_A^I \leq q - 2$ . We choose  $w_A = \frac{\delta_A^R}{2} + i\frac{\delta_A^I - 1}{2}$  and  $w'_A = -\frac{\delta_A^R}{2} - i\frac{\delta_A^I + 1}{2}$ . Therefore, by Definition 1,  $w_A, w'_A \in \mathbb{Z}[i]/q$  since  $w_A^R, w_A^I, w_A'^R, w_A'^I < q/2$ .

P1-4)  $\delta_A^R$  is odd,  $\delta_A^I$  is even

In this case, we choose  $w_A = \frac{\delta_A^R-1}{2} + i\frac{\delta_A^I}{2}$  and  $w'_A = -\frac{\delta_A^R+1}{2} - i\frac{\delta_A^I}{2}$ . Similar to P1-3),  $w_A, w'_A \in \mathbb{Z}[i]/q$ .

**P2)** We consider a complex  $q = q^R + iq^I$  and  $q^R \neq 0$ ,  $q^I \neq 0$ . Since  $q$  is a complex Gaussian prime, we must have  $|q|^2 = (q^R)^2 + (q^I)^2 = 4k + 1$  where  $k$  is an integer. Thus, either  $q^R$  is even and  $q^I$  is odd, or  $q^R$  is odd and  $q^I$  is even. Suppose that  $q^R > q^I \geq 1$ . Thus, the Gaussian integer with the largest magnitude that yields  $|\delta_A| < |q|$  is  $(\delta_A^R, \delta_A^I) = (q^R, q^I - 1)$ .

P2-1)  $q^R$  is even and  $q^I$  is odd

In this case, given  $q^R > q^I \geq 1$ , we further have  $q^R \geq 2$ ,  $q^I \geq 1$ , and  $q^R > q^I$ .

When  $\delta_A = q^R + i(q^I - 1)$ , we let  $w_A = \frac{q^R}{2} + i\frac{q^I-1}{2}$  and  $w'_A = -\frac{q^R}{2} - i\frac{q^I-1}{2}$ . Then,  $\delta_A = w_A - w'_A$ .

Since both  $q^R$  and  $q^I - 1$  are even, by Lemma 15 (as below), both  $w_A, w'_A$  are valid, i.e.,  $w_A, w'_A \in \mathbb{Z}[i]/q$ .

**Lemma 15:** Given a Gaussian integer  $\delta \in \mathbb{Z}[i]$  where  $\delta = \delta^R + i\delta^I$  and a Gaussian prime  $q$  that defines valid symbols in  $\mathbb{Z}[i]$  according to Definition 1. If  $|\delta| < |q|$  and both  $\delta^R, \delta^I$  are even integers, there exists at least one a pair of  $w, w' \in \mathbb{Z}[i]$  such that  $\delta = w - w'$ .

*Proof of Lemma 15:* Since both  $\delta^R, \delta^I$  are even, there exist two Gaussian integers  $w = \frac{\delta^R}{2} + i\frac{\delta^I}{2}$  and  $w' = w - \delta$ . Furthermore, we can verify that  $w, w' \in \mathbb{Z}[i]$ , since  $|w| = |w'| = \frac{\sqrt{(\delta^R)^2 + (\delta^I)^2}}{2} < |q|/2$ . By Proposition 1, both  $w, w' \in \mathbb{Z}[i]$ . ■

P2-2)  $q^R$  is odd and  $q^I$  is even

In this case, given  $q^R > q^I \geq 1$ , we further have  $q^R \geq 3$ ,  $q^I \geq 2$ , and  $q^R > q^I$ .

When  $\delta_A = q^R + i(q^I - 1)$ , we propose to have  $w_A = \frac{q^R+1}{2} + i\frac{q^I-2+2k}{2}$  and  $w'_A = -\frac{q^R-1}{2} - i\frac{q^I+2k}{2}$  for some non-negative integer  $k \geq 0$ , where we will find a suitable  $k$  to ensure both  $w_A$  and  $w'_A$  are valid symbols. We first note that  $\delta_A = w_A - w'_A$ . By Definition 1, the corresponding coordinates of  $w_A$  and  $w'_A$  with the basis  $(x, y)$  are given by

$$\begin{aligned} \begin{bmatrix} w^x \\ w^y \end{bmatrix} &= \frac{1}{|q|} \begin{bmatrix} q^R & q^I \\ -q^I & q^R \end{bmatrix} \begin{bmatrix} \frac{q^R+1}{2} \\ \frac{q^I-2+2k}{2} \end{bmatrix} \\ &= \begin{bmatrix} \frac{|q|}{2} + \frac{q^R-(2+2k)q^I}{2|q|} \\ \frac{-q^I-(2+2k)q^R}{2|q|} \end{bmatrix}, \end{aligned} \quad (122a)$$

$$\begin{aligned} \begin{bmatrix} w'^x \\ w'^y \end{bmatrix} &= \frac{1}{|q|} \begin{bmatrix} q^R & q^I \\ -q^I & q^R \end{bmatrix} \begin{bmatrix} -\frac{q^R-1}{2} \\ -\frac{q^I+2k}{2} \end{bmatrix} \\ &= \begin{bmatrix} -\frac{|q|}{2} + \frac{q^R-2kq^I}{2|q|} \\ \frac{-q^I-2kq^R}{2|q|} \end{bmatrix}. \end{aligned} \quad (122b)$$

To ensure  $|w_A^x|, |w_A^y|, |w'_A^x|, |w'_A^y| < |q|/2$  in (122), we require

$$\begin{aligned} \max \{0, \lfloor \frac{q^R}{2q^I} - 1 \rfloor + 1\} &\leq k \\ &\leq \min \left\{ \lceil \frac{q^R}{2q^I} \rceil - 1, \lceil \frac{|q|^2 - q^I}{2q^R} - 1 \rceil - 1 \right\}, \end{aligned} \quad (123)$$

where  $\lfloor m \rfloor$  is the largest integer that is smaller than  $m$  and  $\lceil m \rceil$  is the smallest integer that is larger than  $m$ . Next, we

verify that there exists at least one non-negative integer  $k$  in (123) such that  $|w_A^x|, |w_A^y|, |w'_A^x|, |w'_A^y| < |q|/2$  (i.e.,  $w_A, w'_A \in \mathbb{Z}[i]/q$ ). Let  $x = \frac{q^R}{2q^I}$  and  $y = \frac{|q|^2 - q^I}{2q^R}$ . In case P2-2) here,  $x$  is not an integer since  $q^R$  is odd. Therefore, we can reduce (123) to

$$\max\{0, \lfloor x \rfloor\} \leq k \leq \min\{\lfloor x \rfloor, \lceil y - 2 \rceil\}, \quad (124)$$

where  $\lfloor x - 1 \rfloor + 1 = \lfloor x \rfloor$  and  $\lceil y - 1 \rceil - 1 = \lceil y - 2 \rceil$ . Note also that  $\lceil x \rceil - 1 = \lfloor x \rfloor$  if  $x$  is not an integer. According to (124), we consider the following possible ranges of  $k$ :

P2-2-i)  $\max\{0, \lfloor x \rfloor\} = 0$  and  $\min\{\lfloor x \rfloor, \lceil y - 2 \rceil\} = \lfloor x \rfloor \Rightarrow 0 \leq k \leq \lfloor x \rfloor$

Since  $\max\{0, \lfloor x \rfloor\} = 0$ , we have  $\lfloor x \rfloor = 0$ . Since  $x$  is positive, it is not possible for  $\lfloor x \rfloor < 0$ . Thus,  $0 \leq k \leq \lfloor x \rfloor$  implies that  $k = 0$  is the only solution. This applies for the case of  $q = 5 + 4i$ .

P2-2-ii)  $\max\{0, \lfloor x \rfloor\} = 0$  and  $\min\{\lfloor x \rfloor, \lceil y - 2 \rceil\} = \lceil y - 2 \rceil \Rightarrow 0 \leq k \leq \lceil y - 2 \rceil$

Since  $\max\{0, \lfloor x \rfloor\} = 0$ , we have  $\lfloor x \rfloor = 0$ . Furthermore, since  $\min\{\lfloor x \rfloor, \lceil y - 2 \rceil\} = \lceil y - 2 \rceil$ , we have  $\lfloor x \rfloor \geq \lceil y - 2 \rceil$ . Given  $q^R \geq 3$  and  $q^I \geq 2$ , we can verify that  $\lceil y - 2 \rceil \geq 0$ , since  $\lceil y - 2 \rceil = \lceil \frac{|q|^2 - q^I}{2q^R} - 2 \rceil = \lceil \frac{q^R}{2} + \frac{q^I(q^I-1)}{2q^R} - 2 \rceil \geq \lceil \frac{3}{2} - 2 \rceil = 0$ . Thus, we have  $\lfloor x \rfloor = \lceil y - 2 \rceil = 0$ . Therefore,  $0 \leq k \leq \lceil y - 2 \rceil$  implies  $k = 0$  is the only solution. This applies for the case of  $q = 3 + 2i$ .

P2-2-iii)  $\max\{0, \lfloor x \rfloor\} = \lfloor x \rfloor$  and  $\min\{\lfloor x \rfloor, \lceil y - 2 \rceil\} = \lfloor x \rfloor \Rightarrow \lfloor x \rfloor \leq k \leq \lfloor x \rfloor$

Thus, we have  $k = \lfloor x \rfloor$  as the only solution. This applies for the case of  $q = 7 + 2i$ .

P2-2-iv)  $\max\{0, \lfloor x \rfloor\} = \lfloor x \rfloor$  and  $\min\{\lfloor x \rfloor, \lceil y - 2 \rceil\} = \lceil y - 2 \rceil \Rightarrow \lfloor x \rfloor \leq k \leq \lceil y - 2 \rceil$

The case where  $\lfloor x \rfloor = 0$  has been dealt with in P2-2-i). Here, we assume  $\lfloor x \rfloor > 0$ . Therefore, we have  $q^R \geq 2q^I$ . However, since  $q^R$  is odd, we must have  $q^R > 2q^I$ . Since  $\min\{\lfloor x \rfloor, \lceil y - 2 \rceil\} = \lceil y - 2 \rceil$ , we have  $\lfloor x \rfloor \geq \lceil y - 2 \rceil$ . Furthermore, given  $q^R \geq 3$ ,  $q^I \geq 2$ , and  $q^R > 2q^I$ , we can verify  $\lfloor x \rfloor \leq \lceil y - 2 \rceil$ . The proof is given as follows:

$$\begin{aligned} \lceil y - 2 \rceil &= \lceil \frac{q^I|q|^2 - (q^I)^2 - (q^R)^2}{2q^Rq^I} - 2 + \frac{(q^R)^2}{2q^Rq^I} \rceil \\ &= \lceil \frac{(q^I - 1)|q|^2 - 4q^Rq^I}{2q^Rq^I} + x \rceil. \end{aligned} \quad (125)$$

When  $q^I > 3$ , given  $q^R > 2q^I$ , we have  $\frac{(q^I-1)|q|^2 - 4q^Rq^I}{2q^Rq^I} > \frac{2|q|^2 - 4q^Rq^I}{2q^Rq^I} > 0$ . Thus,  $\lfloor x \rfloor \leq \lceil y - 2 \rceil$ . When  $q^I = 2$ , given  $q^R > 2q^I$ , we further have

$$\begin{aligned} \lceil y - 2 \rceil &= \lceil \frac{|q|^2 - q^I}{2q^R} - 2 \rceil = \lceil \frac{(q^R)^2 + 2}{2q^R} - 2 \rceil \\ &= \lceil \frac{q^R}{2} + \frac{1}{q^R} - 2 \rceil. \end{aligned} \quad (126)$$

From (126), we have  $\lfloor x \rfloor \leq \lceil y - 2 \rceil$  when  $q^R \geq 8$ . When  $q^R < 8$  and  $q^R$  is odd, the possible  $q^R$  are 5 and 7, since  $q^R > 4$ . In this case of  $q^I = 2$ , we can verify that  $\lfloor x \rfloor = \lceil y - 2 \rceil$  when  $q^R = 5$  and  $\lfloor x \rfloor < \lceil y - 2 \rceil$  when  $q^R = 7$ . The proof of  $\lfloor x \rfloor \leq \lceil y - 2 \rceil$  is completed.

Thus, we have  $\lfloor x \rfloor = \lceil y - 2 \rceil$ , which implies that  $k = \lfloor x \rfloor$  is the only solution. This applies for the case of  $q = 5 + 2i$ .

As we discussed in P2), assuming  $q_A^R > q_A^I \geq 1$ ,  $(\delta_A^R, \delta_A^I) = (q^R, q^I - 1)$  has the largest magnitude that yields  $|\delta_A| < |q|$ . W.l.o.g., the Gaussian integers  $\delta_A$  where  $\delta_A^R, \delta_A^I \geq 0$  with the smaller magnitude, i.e.,  $|\delta_A| < |q^R + i(q^I - 1)|$ , belong to the following subcases:

$$\text{P3)} \delta_A = (q^R - m) + i(q^I - 1 - n);$$

$$\text{P4)} \delta_A = (q^R + m) + i(q^I - 1 - n);$$

$$\text{P5)} \delta_A = (q^R - m) + i(q^I - 1 + n);$$

where  $m, n \geq 1$  and  $n, m \in \mathbb{Z}$  in P3)-P5). The proofs of P3), P4), and P5) are given as follows:

**P3)** We consider  $\delta_A = \delta^R + i\delta^I$  with  $\delta^R = q^R - m$  and  $\delta^I = q^I - 1 - n$ . Suppose that  $\delta^R$  is odd and  $\delta^I$  is odd. We choose  $w_A = \frac{\delta^R+1}{2} + i\frac{\delta^I-1}{2}$  and  $w'_A = -\frac{\delta^R-1}{2} - i\frac{\delta^I+1}{2}$ . Furthermore, we can verify that both  $w_A$  and  $w'_A$  are valid, since  $(\delta^R+1)^2 + (\delta^I)^2 < |q|^2$  in this case. For other subcases in P3) (i.e., even  $\delta^R$  and even  $\delta^I$ , even  $\delta^R$  and odd  $\delta^I$ , odd  $\delta^R$  and even  $\delta^I$ ), the proofs follow similarly.

**P4)** We consider with  $\delta_A = \delta^R + i\delta^I$  with  $\delta^R = q^R + m$  and  $\delta^I = q^I - 1 - n$ . First, we consider the subcase where  $\delta^R$  is even and  $\delta^I$  is odd. In this subcase,  $\delta^R \geq 2$  and  $\delta^I \geq 1$ . W.l.o.g., we assume  $\delta^R, \delta^I \geq 0$ . Furthermore, we deduce that  $n > m$ , since  $q^R > q^I$ . Given that  $\delta^I$  is odd and nonnegative, we have

$$q^I \geq n + 2 \geq m + 1, \quad (127)$$

since  $q^I - n - 1 \geq 1$ . Thus, we have

$$q^R > n + 2, \quad (128)$$

since  $q^R > q^I$ .

Since  $(\delta^R)^2 + (\delta^I)^2 < (q^R)^2 + (q^I - 1)^2$ , we further have  $m^2 + 2q^Rm + n^2 - 2n(q^I - 1) < 0$ , i.e.,  $q^In - q^Rm > \frac{m^2 + n^2 + 2n}{2} > 0$ .

We let  $w = \frac{\delta^R+2k}{2} + i\frac{\delta^I-2j-1}{2}$  and  $w' = -\frac{\delta^R-2k}{2} - i\frac{\delta^I+2j+1}{2}$  where  $k, j \in \mathbb{Z}$ , such that  $\delta = w - w'$ . Then, we have

$$\begin{aligned} \begin{bmatrix} w^x \\ w^y \end{bmatrix} &= \frac{1}{|q|} \begin{bmatrix} q^R & q^I \\ -q^I & q^R \end{bmatrix} \begin{bmatrix} \frac{\delta^R+2k}{2} \\ \frac{\delta^I-2j-1}{2} \end{bmatrix} \\ &= \begin{bmatrix} \frac{q^R(\delta^R+2k)+q^I(\delta^I-2j-1)}{2|q|} \\ \frac{-q^I(\delta^R+2k)+q^R(\delta^I-2j-1)}{2|q|} \end{bmatrix}, \end{aligned} \quad (129a)$$

$$\begin{aligned} \begin{bmatrix} w'^x \\ w'^y \end{bmatrix} &= \frac{1}{|q|} \begin{bmatrix} q^R & q^I \\ -q^I & q^R \end{bmatrix} \begin{bmatrix} -\frac{\delta^R-2k}{2} \\ -\frac{\delta^I+2j+1}{2} \end{bmatrix} \\ &= \begin{bmatrix} \frac{-q^R(\delta^R-2k)-q^I(\delta^I+2j+1)}{2|q|} \\ \frac{q^I(\delta^R-2k)-q^R(\delta^I+2j+1)}{2|q|} \end{bmatrix}. \end{aligned} \quad (129b)$$

To ensure  $|w_A^x|, |w_A^y|, |w'_A^x|, |w'_A^y| < |q|/2$  in (129), we require

$$\frac{q^Rm - q^I(2+n)}{2q^I} < kq^R - jq^I < \frac{q^In - q^Rm}{2q^I}, \quad (130a)$$

$$\frac{-|q|^2 + q^Rn + q^Im}{2q^I} < jq^R + kq^I < \frac{|q|^2 - q^R(n+2) - q^Im}{2} \quad (130b)$$

We can verify that  $(k, j) = (0, 0)$ , i.e.,  $w = \frac{\delta^R}{2} + i\frac{\delta^I-1}{2}$  and  $w' = -\frac{\delta^R}{2} - i\frac{\delta^I+1}{2}$ , is a solution of (130a) and (130b) at the same time. The proof is as follows: First, LHS of (130a) is less than 0 and RHS of (130a) is larger than 0, since  $q^In - q^Rm > 0$ . Second, LHS of (130b) is less than 0 and RHS of (130b) is larger than 0. The proofs of the other subcases in P4) follow similarly. Due to space limit, we omit the derivations here.

**P5)** We consider  $\delta_A = \delta^R + i\delta^I$  with  $\delta^R = q^R - m$  and  $\delta^I = q^I - 1 + n$ . We use the same way in P4) to prove P5), by choosing proper pairs of  $w$  and  $w'$ . Suppose that  $\delta^R$  is even and  $\delta^I$  is odd. We can also verify that  $w = \frac{\delta^R}{2} + i\frac{\delta^I-1}{2}$  and  $w' = -\frac{\delta^R}{2} - i\frac{\delta^I+1}{2}$  are two valid symbols, such that  $\delta_A = w - w'$ .

#### APPENDIX IV - PROOF OF LEMMA 8.2

We prove  $|\tilde{\Xi}| = \sqrt{13}$  only, and the proofs for  $\sqrt{17}, \sqrt{29}, \sqrt{37}$  follow similarly.

W.l.o.g., consider  $\tilde{\Xi} = 3 + 2i$  (the treatment of other  $\tilde{\Xi}$  with  $|\tilde{\Xi}|^2 = 13$  is similar). First, we express  $\kappa, \tau, \gamma, \delta$  in the form of a quotient and a remainder as in (58). Then, we have

$$\begin{aligned} &\kappa\delta - \tau\gamma \\ &= \tilde{\Xi}^2(q_\kappa q_\delta - q_\tau q_\gamma) + \tilde{\Xi}[(q_\kappa r_\delta + q_\delta r_\kappa) - (q_\tau r_\gamma + q_\gamma r_\tau)] \\ &\quad + (r_\kappa r_\delta - r_\tau r_\gamma) = \tilde{\Xi}. \end{aligned} \quad (131)$$

We see that in order that the last equality in (131) applies, we must have  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ . Since  $\tilde{\Xi}$  is Gaussian-integer prime in this case, finite-field arithmetic applies to the remainders. The elements in the field  $\mathbb{Z}[i]/(3 + 2i)$  are  $\{0, \epsilon, \epsilon(1 + i), 2\epsilon\}$ , where  $\epsilon$  is a unit.

Given  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$  as implied by (131), there are three possibilities as follows:

- (p1)  $r_\kappa, r_\tau, r_\gamma, r_\delta$  are all nonzero;
- (p2)  $r_\kappa = r_\gamma = 0, r_\tau, r_\delta \neq 0$ ;
- (p3)  $r_\tau = r_\delta = 0, r_\kappa, r_\gamma \neq 0$ .

Note that it is not possible for  $r_\kappa = r_\tau = 0$  because that would imply  $\gcd(\kappa, \tau) \neq 1$  according to (131). Similarly, it is not possible for  $r_\gamma = r_\delta = 0$ .

We can write (77a) and (77b) as

$$\begin{aligned} \tilde{\Xi}\phi &= \zeta\kappa + \vartheta\gamma = \tilde{\Xi}(\zeta q_\kappa + \vartheta q_\gamma) + (\zeta r_\kappa + \vartheta r_\gamma), \\ \tilde{\Xi}\psi &= \zeta\tau + \vartheta\delta = \tilde{\Xi}(\zeta q_\tau + \vartheta q_\delta) + (\zeta r_\tau + \vartheta r_\delta). \end{aligned} \quad (132)$$

Then, we let  $\zeta = 1$  and rewrite (132) as

$$\begin{aligned} \tilde{\Xi}\phi &= \kappa + \vartheta\gamma = \tilde{\Xi}(q_\kappa + \vartheta q_\gamma) + (r_\kappa + \vartheta r_\gamma), \\ \tilde{\Xi}\psi &= \tau + \vartheta\delta = \tilde{\Xi}(q_\tau + \vartheta q_\delta) + (r_\tau + \vartheta r_\delta). \end{aligned} \quad (133)$$

To satisfy (133), we further let

$$\begin{aligned} \vartheta &= -r_\kappa r_\gamma^{-1} = -r_\tau r_\delta^{-1} \pmod{\tilde{\Xi}} \text{ (if (p1) above applies);} \\ \vartheta &= -r_\tau r_\delta^{-1} \pmod{\tilde{\Xi}} \text{ (if (p2) above applies);} \\ \vartheta &= -r_\kappa r_\gamma^{-1} \pmod{\tilde{\Xi}} \text{ (if (p3) above applies).} \end{aligned} \quad (134)$$

Given  $\zeta = 1$ , if  $\vartheta \in \{\epsilon, \epsilon(1 + i)\}$  in (134), (77c) is satisfied, since  $0 < 1 + |\vartheta| \leq \sqrt{\frac{13}{2}}$ . On the other hand, if  $\vartheta \in \{2\epsilon\}$ ,

(77c) cannot be satisfied, since  $1 + |\vartheta| > \sqrt{\frac{13}{2}}$ . Note that if  $\vartheta \in \{2\epsilon\}$ , then  $\vartheta^{-1} \in \{\epsilon(1+i)\}$ . So, we multiply (133) by  $\vartheta^{-1}$  so that  $\zeta$  becomes  $\vartheta^{-1}$  and  $\vartheta$  becomes 1 in (133). Doing (2-iii) so gives us:

$$\begin{aligned}\tilde{\Xi}\phi &= \zeta\kappa + \gamma = \tilde{\Xi}(\zeta q_\kappa + q_\gamma) + (\zeta r_\kappa + r_\gamma), \\ \tilde{\Xi}\psi &= \zeta\tau + \delta = \tilde{\Xi}(\zeta q_\tau + q_\delta) + (\zeta r_\tau + r_\delta).\end{aligned}\quad (135)$$

where  $\zeta = -r_\delta r_\tau^{-1}$  and/or  $-r_\gamma r_\kappa^{-1} \pmod{\tilde{\Xi}}$ . Then, we can verify that (77b) is satisfied.

Therefore, we have proved *Lemma 8.2* under  $|\tilde{\Xi}|^2 = 13$ .

#### APPENDIX V - PROOF OF LEMMA 8.3

W.l.o.g., we consider  $\tilde{\Xi} = 3 + i = -i(1+i)(1+2i)$ . First, we express  $\kappa, \tau, \gamma, \delta$  in the form of a quotient and a remainder as in (58). Eqn. (131) is still valid, and we also have  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ . The remainders  $r_\kappa, r_\tau, r_\gamma, r_\delta \in \mathbb{Z}[i]/(3+i) = \{0, \epsilon, \epsilon(1+i), 1+2i\}$ , where  $\epsilon$  is a unit.

Case 1: One of the remainders is 0

W.l.o.g., suppose that  $r_\kappa = 0$ . By *Lemma 8.3.1* (presented later), we cannot have  $r_\tau = 0$  or  $\epsilon(1+i)$  or  $(1+2i)$ . Therefore,  $r_\tau = \epsilon$ . Then,  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$  implies  $r_\gamma = 0$ . Now, since  $r_\gamma = 0$ , by *Lemma 8.3.1*,  $r_\delta = v$  for some  $v \in \{\pm 1, \pm i\}$ . Overall, we have  $r_\kappa = r_\gamma = 0$ ,  $r_\tau = \epsilon$ , and  $r_\delta = v$ . We can write (79a) and (79b) as

$$\tilde{\Xi}\phi = \zeta\kappa + \vartheta\gamma = \tilde{\Xi}(\zeta q_\kappa + \vartheta q_\gamma) + (\zeta r_\kappa + \vartheta r_\gamma), \quad (136a)$$

$$\tilde{\Xi}\psi = \zeta\tau + \vartheta\delta = \tilde{\Xi}(\zeta q_\tau + \vartheta q_\delta) + (\zeta r_\tau + \vartheta r_\delta). \quad (136b)$$

A way to satisfy (136) is to let  $\zeta = r_\delta = v$ ,  $\vartheta = -r_\tau = -\epsilon$ . We see that  $|\zeta| + |\vartheta| = 2 < \frac{|\tilde{\Xi}|}{\sqrt{2}} = \frac{\sqrt{10}}{\sqrt{2}}$  satisfying (79c). Now, we see that the only possible way for  $(\phi, \psi) = (0, 0)$  is for  $(\kappa, \tau) = \frac{\epsilon}{v}(\gamma, \delta)$ . However, this contradicts our statement that  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$ . Therefore,  $(\phi, \psi) \in \mathbb{Z}^2[i] \setminus \{(0, 0)\}$ .

Case 2: No remainder is 0, and one remainder is a unit.

W.l.o.g., suppose that  $r_\kappa$  is a unit and  $r_\kappa = 1$ . Then, from (131), we have  $r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ ,  $r_\tau, r_\gamma, r_\delta \in \{\epsilon, \epsilon(1+i), 1+2i\}$ .

(2-i)  $r_\delta = \text{unit}$

Suppose that  $r_\delta = \epsilon, \epsilon \in \{\pm 1, \pm i\}$ , giving  $\epsilon = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ . We can verify that for this case, both  $r_\tau$  and  $r_\gamma$  must also be units (otherwise,  $r_\tau r_\gamma$  is not congruent to a unit  $\pmod{\tilde{\Xi}}$ ). Overall, all remainders are units. W.l.o.g., we let  $r_\gamma = \omega$  and  $r_\tau = v$ , where  $\omega, v$  are units. Then we have  $\epsilon = \omega v$ . Again, with the writing of (79a) and (79b) as (132), we can let  $\zeta = r_\delta = \epsilon$ ,  $\vartheta = -r_\tau = -v$  to satisfy (132). The rest is the same as the last part of case 1.

(2-ii)  $r_\delta = \epsilon(1+i)$ , where  $\epsilon \in \{\pm 1, \pm i\}$

In this case,  $r_\delta = \epsilon(1+i) = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ . By *Lemma 8.3.1*, given  $r_\delta = \epsilon(1+i)$ , then  $r_\gamma \neq v(1+i), \forall v \in \{\pm 1, \pm i\}$ . We can also rule out the possibility of  $r_\gamma = v(1+2i)$  and  $r_\tau = v(1+i)$  where  $v$  denotes any unit, since  $(1+i)(1+2i) = 0 \pmod{\tilde{\Xi}}$ .

Furthermore, we can verify that the way to satisfy  $r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$  is for  $r_\gamma = \omega$ ,  $r_\tau = v(1+i)$ , and  $\epsilon = \omega v$ , where  $\omega, v$  are both units. Overall,  $r_\kappa = 1$ ,  $r_\tau = v(1+i)$ ,  $r_\gamma = \omega$ , and  $r_\delta = \epsilon(1+i)$ . To satisfy (132), we can

let  $\zeta = 1, \vartheta = -\epsilon^{-1}v$ . The rest is the same as the last part of case 1.

$r_\delta = 1 + 2i$

Although by the relationship  $r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ , it is possible for  $r_\gamma = r_\tau = 1 + 2i$  (because  $(1+2i)^2 = (1+2i) \pmod{\tilde{\Xi}}$ ). However, this possibility is ruled out because it will violate  $\gcd(\gamma, \delta) = 1$ . The only possibility is  $r_\tau = 1 + 2i$  and  $r_\gamma = 1$ . Overall, we have  $r_\kappa = 1$ ,  $r_\tau = 1 + 2i$ ,  $r_\gamma = 1$ , and  $r_\delta = 1 + 2i$ . The rest is the same as the last part of case 1.

Case 3: No remainder is 0 or a unit, one remainder is  $\epsilon(1+i)$ .

W.l.o.g., suppose that  $r_\kappa = 1 + i$ . Then,  $r_\tau = 1 + 2i$  by *Lemma 8.3.1*. Then,  $(1+i)r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$  means  $r_\gamma = 1 + i$  and  $r_\delta = 1 + 2i$ . To satisfy (132), we can let  $\zeta = 1$  and  $\vartheta = -1$ . The rest is the same as the last part of subcase 1.

Subcase 4: No remainder is 0 or a unit, or  $\epsilon(1+i)$ , all remainders are  $1 + 2i$ .

This case is obviously not possible because of the requirement  $\gcd(\kappa, \tau) = \gcd(\gamma, \delta) = 1$ .

Therefore, we have proved *Lemma 8.3* under  $|\tilde{\Xi}|^2 = 10$ .

*Lemma 8.3.1:* With respect the proof in *Lemma 8.3*, given  $\gcd(\kappa, \tau) = \gcd(\gamma, \delta) = 1$  and  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ , for  $\Xi = 3 + i = -i(1+i)(1+2i)$ , the following are not possible:

$(r_\kappa = 0 \text{ or } \epsilon(1+i))$  and  $(r_\tau = 0 \text{ or } v(1+i))$ ;

$(r_\gamma = 0 \text{ or } \epsilon(1+i))$  and  $(r_\delta = 0 \text{ or } v(1+i))$ ;

$(r_\kappa = 0 \text{ or } 1+2i)$  and  $(r_\tau = 0 \text{ or } 1+2i)$ ;

$(r_\gamma = 0 \text{ or } 1+2i)$  and  $(r_\delta = 0 \text{ or } 1+2i)$ ;

where  $\epsilon, v \in \{\pm 1, \pm i\}$  denote some arbitrary units.

*Proof of Lemma 8.3.1:*

Each of the cases in the above is disallowed because it will lead to  $\gcd(\kappa, \tau) \neq 1$  or  $\gcd(\gamma, \delta) \neq 1$ . For example, if  $r_\kappa = 0$  or  $(1+i)$ ,  $r_\tau = -(1+i)$ , then  $\gcd(\kappa, \tau) = 1 + i$ . ■

#### APPENDIX VI - PROOF OF LEMMA 8.4

The representative elements of  $\mathbb{Z}[i]/5$  are  $\{0, \epsilon, \epsilon(1+i), 2\epsilon, \epsilon(2+i), \epsilon(2-i), \epsilon(2+2i)\}$ , where  $\epsilon \in \{\pm 1, \pm i\}$ . From Fig. 14, we see that the non-zero elements other than  $\epsilon(2+i)$  and  $\epsilon(2-i)$  all have inverses.

We express  $\kappa, \tau, \gamma, \delta$  in the form of a quotient and a remainder with division by  $\Xi = 5$ , as in (58). Eqn. (131) is still valid, and we also have  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ . The remainders  $r_\kappa, r_\tau, r_\gamma, r_\delta \in \mathbb{Z}[i]/5 = \{0, \epsilon, \epsilon(1+i), 2\epsilon, \epsilon(2+i), \epsilon(2-i), \epsilon(2+2i)\}$ .

Case 1:  $r_\kappa, r_\tau, r_\gamma, r_\delta \in \{\epsilon, \epsilon(1+i), 2\epsilon, \epsilon(2+2i)\}$

In this case, since inverses of  $r_\kappa, r_\gamma, r_\tau, r_\delta$  exists, we can apply the same argument as in the proof of the case of  $|\Xi| = \sqrt{13}$ . Note that  $\vartheta \notin \{\epsilon(2+i), \epsilon(2-i)\}$ , according to the multiplication in Fig. 14. In case  $\vartheta = \epsilon(2+2i)$ , we do a transformation to make  $\zeta = \vartheta^{-1} = v(1+i)$ ,  $v$  is unit, and  $\vartheta = 1$ . Thus, we can make sure

$$|\zeta| + |\vartheta| \leq 1 + \sqrt{2} < \frac{5}{\sqrt{2}} = \frac{|\Xi|}{\sqrt{2}}. \quad (137)$$

Case 2: One of  $r_\kappa, r_\tau, r_\gamma, r_\delta$  is 0

W.l.o.g., suppose that  $r_\kappa = 0$ . Then,  $r_\tau \notin \{0, \epsilon(2+i), \epsilon(2-i)\}$  because  $\gcd(\kappa, \tau) = 1$ . Given that  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\Xi}$ ,

$\bullet$	$\varepsilon_2$	$\varepsilon_2(1+i)$	$2\varepsilon_2$	$\varepsilon_2(2+i)$	$\varepsilon_2(2-i)$	$\varepsilon_2(2+2i)$
$\varepsilon_1$	$\varepsilon_1\varepsilon_2$	$\varepsilon_1\varepsilon_2(1+i)$	$2\varepsilon_1\varepsilon_2$	$\varepsilon_1\varepsilon_2(2+i)$	$\varepsilon_1\varepsilon_2(2-i)$	$\varepsilon_1\varepsilon_2(2+2i)$
$\varepsilon_1(1+i)$	$\varepsilon_1\varepsilon_2(1+i)$	$2\varepsilon_1\varepsilon_2i$	$\varepsilon_1\varepsilon_2(2+2i)$	$-i\varepsilon_1\varepsilon_2(2+i)$	$-\varepsilon_1\varepsilon_2(2-i)$	$-\varepsilon_1\varepsilon_2i$
$2\varepsilon_1$	$2\varepsilon_1\varepsilon_2$	$\varepsilon_1\varepsilon_2(2+2i)$	$-\varepsilon_1\varepsilon_2$	$i\varepsilon_1\varepsilon_2(2+i)$	$-i\varepsilon_1\varepsilon_2(2-i)$	$-\varepsilon_1\varepsilon_2(1+i)$
$\varepsilon_1(2+i)$	$\varepsilon_1\varepsilon_2(2+i)$	$-i\varepsilon_1\varepsilon_2(2+i)$	$i\varepsilon_1\varepsilon_2(2+i)$	$-\varepsilon_1\varepsilon_2(2+i)$	0	$\varepsilon_1\varepsilon_2(2+i)$
$\varepsilon_1(2-i)$	$\varepsilon_1\varepsilon_2(2-i)$	$-\varepsilon_1\varepsilon_2(2-i)$	$-i\varepsilon_1\varepsilon_2(2-i)$	0	$-\varepsilon_1\varepsilon_2(2-i)$	$i\varepsilon_1\varepsilon_2(2-i)$
$\varepsilon_1(2+2i)$	$\varepsilon_1\varepsilon_2(2+2i)$	$-\varepsilon_1\varepsilon_2i$	$-\varepsilon_1\varepsilon_2(1+i)$	$\varepsilon_1\varepsilon_2(2+i)$	$i\varepsilon_1\varepsilon_2(2-i)$	$-2\varepsilon_1\varepsilon_2i$

Fig. 14. Multiplication for non-zero elements in  $\mathbb{Z}[i]/5$ , where  $\varepsilon_1$  and  $\varepsilon_2$  are units.

we must have  $r_\gamma = 0$ . Given  $r_\gamma = 0$ ,  $r_\delta \notin \{0, \varepsilon(2+i), \varepsilon(2-i)\}$ . Thus, inverses of  $r_\tau, r_\delta$  exist. We can choose  $\zeta = 1, \vartheta = -r_\tau r_\delta^{-1}$  if  $-r_\tau r_\delta^{-1} \neq \varepsilon(2+2i)$ ; and  $\zeta = -r_\tau^{-1} r_\delta, \vartheta = 1$  otherwise. The statement of the lemma is thus fulfilled.

Case 3: One of  $r_\kappa, r_\tau, r_\gamma, r_\delta$  is  $\varepsilon(2+i)$ , none of  $r_\kappa, r_\tau, r_\gamma, r_\delta$  is 0

W.l.o.g., suppose that  $r_\kappa = \varepsilon(2+i)$ . Then,  $r_\tau \neq v(2+i)$  because  $\gcd(\kappa, \tau) = 1$ . Given that  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\Xi}$  and  $r_\kappa = \varepsilon(2+i)$ ,  $r_\tau \notin \{0, v(2+i)\}$ ,  $r_\delta \neq 0$ , we must have  $r_\gamma = v(2+i)$  for some unit  $v$ , according to Fig. 14. That  $r_\gamma = v(2+i)$  also means  $r_\delta \neq \omega(2+i)$ , where  $\omega$  is a unit. Overall, we have the following possibilities:  $r_\kappa = \varepsilon(2+i), r_\gamma = v(2+i), r_\tau, r_\delta \in \{\varepsilon, \varepsilon(1+i), \varepsilon(2-i), \varepsilon(2+2i)\}$ .

(3-i)  $r_\tau, r_\delta \neq \varepsilon(2-i)$

In this subcase, both  $r_\tau, r_\delta$  have an inverse. We can choose  $\zeta = 1, \vartheta = -r_\tau r_\delta^{-1}$  if  $-r_\tau r_\delta^{-1} \neq \varepsilon(2+2i)$ ; and  $\zeta = -r_\tau^{-1} r_\delta, \vartheta = 1$  otherwise. This ensures  $\zeta r_\tau + \vartheta r_\delta = 0 \pmod{5}$  (note that  $r_\kappa r_\delta - r_\tau r_\gamma = 0 \pmod{\Xi} \Rightarrow \zeta, \vartheta$  selected above are such that  $\zeta r_\tau + \vartheta r_\delta = 0 \pmod{5}$ ). Overall, we also have  $|\zeta| + |\vartheta| \leq 1 + \sqrt{2} < \frac{5}{\sqrt{2}} = \frac{|\Xi|}{\sqrt{2}}$ .

(3-ii) One of  $r_\tau, r_\delta = \varepsilon(2-i)$

W.l.o.g., suppose that  $r_\tau = \omega(2-i)$ . Then,  $r_\kappa r_\delta - r_\tau r_\gamma = 0 \pmod{\Xi} \Rightarrow \varepsilon(2+i)r_\delta - \omega(2-i)v(2+i) = 0 \pmod{\Xi}$ . Therefore, we have  $r_\delta = \mu(2-i)$ , where  $\mu$  is a unit. We want to find  $\zeta, \vartheta$  such that

$$\kappa\zeta + \gamma\vartheta = 0 \pmod{5}, \quad (138a)$$

$$\tau\zeta + \delta\vartheta = 0 \pmod{5}, \quad (138b)$$

$$0 < |\zeta| + |\vartheta| \leq \frac{5}{\sqrt{2}}. \quad (138c)$$

Substituting the above values of  $r_\kappa, r_\gamma, r_\tau, r_\delta$  and setting  $\vartheta = 1$  in (138a) and (138b), we have

$$\varepsilon[\zeta(2+i) + \varepsilon^{-1}v(2+i)] = 0 \pmod{5}, \quad (139a)$$

$$\omega[\zeta(2-i) + \omega^{-1}\mu(2-i)] = 0 \pmod{5}. \quad (139b)$$

If  $\varepsilon^{-1}v = \omega^{-1}\mu$ , then we just set  $\zeta = -\varepsilon^{-1}v$ , giving  $0 < |\zeta| + |\vartheta| = 1 + 1 \leq \frac{5}{\sqrt{2}}$ .

If  $\varepsilon^{-1}v = -\omega^{-1}\mu$ , we note from Fig. 14 that multiplying  $(2+i)$  by 2 is the same as the multiplying it by  $i$ ; and multiplying  $(2-i)$  by 2 is the same as multiplying it by  $-i$ . Accordingly, we set  $\zeta = -\varepsilon^{-1}v \cdot -i \cdot 2$ . This fulfills (139). We have  $0 < |\zeta| + |\vartheta| = 2 + 1 \leq \frac{5}{\sqrt{2}}$ .

If  $\varepsilon^{-1}v = i\omega^{-1}\mu$ , we note from Fig. 14 that multiplying  $(2+i)$  by  $(1+i)$  is the same as the multiplying it by  $-i$ ; and multiplying  $(2-i)$  by  $(1+i)$  is the same as multiplying it by  $-1$ . Accordingly, we set  $\zeta = -\varepsilon^{-1}v \cdot i \cdot (1+i)$ . This fulfills (139). We have  $0 < |\zeta| + |\vartheta| = \sqrt{2} + 1 \leq \frac{5}{\sqrt{2}}$ .

If  $\varepsilon^{-1}v = -i\omega^{-1}\mu$ , we take the complex conjugates on both sides to get  $\varepsilon v^{-1} = i\omega\mu^{-1}$ . Instead of setting  $\vartheta = 1$ , we set  $\zeta = 1$ , and instead of (139), we have

$$v[\varepsilon v^{-1}(2+i) + \vartheta(2+i)] = 0 \pmod{5}, \quad (140a)$$

$$\mu[\omega\mu^{-1}(2-i) + \vartheta(2-i)] = 0 \pmod{5}. \quad (140b)$$

We then set  $\vartheta = -\varepsilon v^{-1} \cdot i \cdot (1+i)$ . We again have  $0 < |\zeta| + |\vartheta| = \sqrt{2} + 1 \leq \frac{5}{\sqrt{2}}$ .

This completes the proof of subcase (3-ii).

Case 4: One of  $r_\kappa, r_\gamma, r_\tau, r_\delta$  is  $\varepsilon(2-i)$ , none of  $r_\kappa, r_\gamma, r_\tau, r_\delta$  is 0

The proof of case 4 is similar to case 3 by symmetry.

## APPENDIX VII - PROOF OF LEMMA 10

This proof consists two parts. First, Part 1 proves that there exists  $(\zeta, \vartheta)$  such that (65a) and (65b) are satisfied. Then, Part 2 proves that  $(\phi, \psi)$  satisfying (65a) and (65b) is a distance-valid difference pair, i.e.,  $(\phi, \psi) \in \Delta$ .

*Remark:* In this proof, we will not follow *Lemmas 8.1-8.4* to prove (65c), since  $(\zeta, \vartheta)$  yielding (65a) and (65b) cannot satisfy (65c) for the case of  $|\tilde{\Xi}| = 2$  or 3.

### Part 1:

(1)  $|\tilde{\Xi}| = 2$

W.l.o.g., we consider  $\tilde{\Xi} = 2 = (1+i)(1-i)$ . First, we express  $\kappa, \tau, \gamma, \delta$  in the form of a quotient and a remainder as in (58). Eqn. (131) is still valid, and we also have  $r_\kappa r_\delta = r_\tau r_\gamma \pmod{\tilde{\Xi}}$ . The remainders  $r_\kappa, r_\tau, r_\gamma, r_\delta \in \mathbb{Z}[i]/2 = \{0, 1, i, 1+i\}$ .

Case 1: One of the remainders is 0

W.l.o.g., suppose that  $r_\kappa = 0$ . Since  $\gcd(\kappa, \tau) = 1$ ,  $r_\tau \notin \{0, 1+i\}$ . Therefore,  $r_\tau = 1$  or  $i$ .

(1-i)  $r_\tau = 1$

In this subcase, the only possibility for  $0 = r_\gamma \pmod{2}$  is  $r_\gamma = 0$ . Given  $r_\gamma = 0$ , we have  $r_\gamma \in \{0, 1, i, 1+i\}$ . However, we can rule out the possibility of  $r_\gamma = 1+i$ , since this contradicts  $\gcd(\gamma, \delta) = 1$ . Therefore, we have  $r_\delta = 1$  or  $i$ . Overall, we have  $r_\kappa = 0, r_\tau = 1, r_\gamma = 0$ , and



$r_\delta \in \{1, i\}$ . To satisfy (131), if  $r_\delta = 1$ , we can choose  $\zeta = 1, \vartheta = \pm 1$ , where the sign of  $\vartheta$  does not matter (i.e., both signs will work); if  $r_\delta = i$ , we can choose  $\zeta = 1, \vartheta = \pm i$ , where the sign of  $\vartheta$  does not matter.

(1-ii)  $r_\tau = i$

This subcase is similar to subcase (1-i). We can also either choose  $\zeta = 1, \vartheta = \pm 1$  or  $\zeta = 1, \vartheta = \pm i$ .

Case 2: No remainder is 0, one remainder is 1.

W.l.o.g., suppose that  $r_\kappa = 1$ . Since  $\gcd(\gamma, \delta) = 1$ ,  $r_\tau \in \{1, i, 1+i\}$ .

(2-i)  $r_\tau = 1$

Since  $r_\delta = r_\gamma \pmod{2}$ , we have  $(r_\gamma, r_\delta) \in \{(1, 1), (i, i), (1+i, 1+i)\}$ . However, since  $\gcd(\gamma, \delta) = 1$ , we can rule out the possibility of  $(r_\gamma, r_\delta) = (1+i, 1+i)$ . If  $(r_\gamma, r_\delta) = (1, 1)$ , we choose  $\zeta = 1, \vartheta = \pm 1$ , where the sign of  $\vartheta$  does not matter. If  $(r_\gamma, r_\delta) = (i, i)$ , we choose  $\zeta = 1, \vartheta = \pm i$ , where the sign of  $\vartheta$  does not matter.

(2-ii)  $r_\tau = i$

This subcase is similar to subcase (2-i).

(2-iii)  $r_\tau = 1+i$

Since  $r_\delta = (1+i)r_\gamma \pmod{2}$ , we have  $(r_\gamma, r_\delta) \in \{(1, 1+i), (i, 1+i)\}$ . If  $(r_\gamma, r_\delta) = (i, 1+i)$ , we choose  $\zeta = 1, \vartheta = \pm 1$ , where the sign of  $\vartheta$  does not matter. If  $(r_\gamma, r_\delta) = (1, 1+i)$ , we choose  $\zeta = 1, \vartheta = \pm i$ , where the sign of  $\vartheta$  does not matter.

Case 3: No remainder is 0 or 1, one remainder is  $i$ .

W.l.o.g., suppose that  $r_\kappa = i$ . Since  $\gcd(\gamma, \delta) = 1$ ,  $r_\tau \in \{i, 1+i\}$ .

(3-i)  $r_\tau = i$

Since  $ir_\delta = ir_\gamma \pmod{2}$ , we have  $(r_\gamma, r_\delta) \in \{(i, i), (1+i, 1+i)\}$ . However, since  $\gcd(\gamma, \delta) = 1$ , we can rule out the possibility of  $(r_\gamma, r_\delta) = (1+i, 1+i)$ . Overall, we have  $r_\kappa = i, r_\tau = i, r_\gamma = i$ , and  $r_\delta = i$ . To satisfy (131), we choose  $\zeta = 1, \vartheta = \pm 1$ , where the sign of  $\vartheta$  does not matter.

(3-ii)  $r_\tau = 1+i$

In this subcase, the only possibility for  $ir_\delta = (1+i)r_\gamma \pmod{2}$  is  $(r_\gamma, r_\delta) = (i, 1+i)$ . Overall, we have  $r_\kappa = i, r_\tau = 1+i, r_\gamma = i$ , and  $r_\delta = 1+i$ . To satisfy (131), we choose  $\zeta = 1, \vartheta = \pm 1$ , where the sign of  $\vartheta$  does not matter.

Case 4: No remainder is 0 or 1 or  $i$ , all remainders are  $1+i$ .

W.l.o.g., suppose that  $r_\kappa = 1+i$ . However, this subcase is not possible because of the requirement  $\gcd(\kappa, \tau) = 1$ .

For all of cases 1, 2, and 3 above, one of the following two choices must be able to satisfy (65a) and (65b):

*Choice 1:* we can choose either  $\zeta = 1, \vartheta = 1$  or  $\zeta = 1, \vartheta = -1$  (specifically, the sign of  $\vartheta$  does not matter; both  $\vartheta = 1$  and  $\vartheta = -1$  will work if this choice is the valid choice);

*Choice 2:* we can choose either  $\zeta = 1, \vartheta = i$  or  $\zeta = 1, \vartheta = -i$  (again, the sign of  $\vartheta$  does not matter here);

Since  $(\kappa, \tau) \neq (\nu\gamma, \nu\delta)$  where  $\nu = \pm 1$  or  $\pm i$  from the statement of the lemma, we have  $\phi \neq 0$  and  $\psi \neq 0$ .

(2)  $|\tilde{\Xi}| = 3$

With a proof substantially similar in spirit to that of  $|\tilde{\Xi}| = 2$ , we can show that one of the following three choices will satisfy (65a) and (65b) for  $|\tilde{\Xi}| = 3$ :

*Choice 1:* we can choose either  $\zeta = 1, \vartheta = 1$  or  $\zeta = 1, \vartheta = -1$ ;

*Choice 2:* we can choose either  $\zeta = 1, \vartheta = i$  or  $\zeta = 1, \vartheta = -i$ ;

*Choice 3:* we can choose either  $\zeta = 1, \vartheta = 1+i$  or  $\zeta = 1, \vartheta = -1-i$ ;

Again, for the valid choice, the sign of  $\vartheta$  does not matter here.

## Part 2:

We first prove  $|\tilde{\Xi}| = 2$ . In the following, we prove the case where *Choice 1* is the valid choice to satisfy (65a) and (65b). Similar proof applies if *Choice 2* is the valid choice.

Given *Choice 1*, we first show that there exists  $(\phi, \psi) = (\frac{\kappa+\vartheta\gamma}{\tilde{\Xi}}, \frac{\tau+\vartheta\delta}{\tilde{\Xi}}) \in \Delta$  (i.e.,  $(\phi, \psi)$  is a distance-valid pair). According to the convex regions in *Definition 13*, we introduce a property of convex regions, as follows:

*Convex Combination [29]:* Given  $\sum_k a_k \leq 1$  where  $a_k \geq 0$ , and  $\forall c_k \in \mathcal{G}_q$ , we have  $\sum_k a_k c_k \in \mathcal{G}_q$ . ■

*Statement 1:* If  $a$  is a valid difference (i.e.,  $a \in \Lambda$ ), so is  $i^n a, \forall n \in \{1, 2, 3\}$ . Similarly, if  $b \in \mathcal{G}_q$ , then  $i^n b \in \mathcal{G}_q, \forall n \in \{1, 2, 3\}$ . ■

The proof of *Statement 1* is given as follows. If  $a \in \Lambda$ , we can find  $w, w' \in \mathbb{Z}[i]/q$  such that  $a = w - w'$ . Then,  $i^n a = i^n(w - w') \in \Lambda$  for  $n \in \{1, 2, 3\}$ , since  $i^n w, i^n w' \in \mathbb{Z}[i]/q$  by *Definition 1*.

Since  $b \in \mathcal{G}_q$ , we have  $b = \sum_{k=1}^K a_k c_k$ , where  $\sum_k a_k \leq 1$ ,  $a_k \geq 0$ , and  $\forall c_k \in \mathcal{G}_q$ . Then,  $i^n b = \sum_{k=1}^K a_k (i^n c_k)$ . Given  $c_k \in \Lambda$ ,  $i^n c_k$  is also a valid difference as we proved above. Therefore,  $i^n b \in \mathcal{G}_q$ , since  $i^n b$  is also a convex combination.

*Statement 2:* When  $\tilde{\Xi} = 2$ , for any  $\kappa, \gamma \in \Lambda$ ,  $\phi = \frac{\kappa+\vartheta\gamma}{\tilde{\Xi}} \in \Lambda$ , where  $\vartheta$  can be 1 or  $-1$ . ■

Proof of *Statement 2* is given as follows. By *Statement 1*,  $\epsilon\gamma \in \mathcal{G}_q$ , where  $\epsilon$  can be any unit. Since convex region is closed under linear combination, we have  $\phi \in \mathcal{G}_q$ . Therefore, by *Lemma 9*, we have  $\phi \in \Lambda$ . Similarly, we can also prove that  $\psi \in \Lambda$ .

Suppose that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent under  $\tilde{\Xi} = \kappa\delta - \tau\gamma = 2$ . The following part is similar to the proof in (67). If  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent, then there exists a common point  $z'$  equidistant to  $(\kappa, \tau)$  and  $(\gamma, \delta)$  such that no other generators are closer to  $z'$  than are  $(\kappa, \tau)$  and  $(\gamma, \delta)$ . From (65a) and (65b), the weighted distance from  $(\phi, \psi)$  to  $z'$  is

$$|\psi z' - \phi| = \frac{|(\tau z' - \kappa) + \vartheta(\delta z' - \gamma)|}{2}, \quad (141)$$

where  $\vartheta$  can be 1 or  $-1$  in *Choice 1*.

Then, we have

$$\begin{aligned} & |(\tau z' - \kappa) + \vartheta(\delta z' - \gamma)| \\ &= \sqrt{|\tau z' - \kappa|^2 + |\vartheta(\delta z' - \gamma)|^2 - 2|\tau z' - \kappa||\vartheta(\delta z' - \gamma)| \cos \theta_\vartheta} \\ &= \sqrt{2|\tau z' - \kappa|^2(1 - \cos \theta_\vartheta)} \leq \sqrt{2}|\tau z' - \kappa|, \end{aligned} \quad (142)$$

where  $\theta_\vartheta$  denote the angle between two vectors  $\tau z' - \kappa$  and  $\vartheta(\delta z' - \gamma)$ . Note that  $\theta_\vartheta$  depends on  $\vartheta$ . Furthermore, the first equality holds because of *cosine rule*, the second equality

holds because of  $|\tau z' - \kappa| = |\vartheta(\delta z' - \gamma)|$ , and the inequality holds since we can either choose  $\vartheta = 1$  or  $-1$  such that  $0 < \theta_\vartheta \leq 90^\circ$  yielding  $|1 - \cos \theta| \leq 1$ .

From (141) and (142), we further have

$$|\psi z' - \phi| < \frac{\sqrt{2}}{2} |\tau z' - \kappa| < |\tau z' - \kappa|. \quad (143)$$

Obviously, (143) contradicts our assumption that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are adjacent.

The proof of  $|\tilde{\Xi}| = 3$  follows similarly. First, by *Statement 1* and *Lemma 9*, we can also show that  $\phi = \frac{\kappa + \vartheta \gamma}{\Xi} \in \Lambda$  where  $\vartheta$  is chosen from any choice in Part I. Second, we follow the proof by contradiction in (141) and (142). For example, suppose that *Choice 3*, where  $\vartheta = 1 + i$  or  $-1 - i$ , is the valid choice. Then,  $|(\tau z' - \kappa) + \vartheta(\delta z' - \gamma)| = \sqrt{3} |\tau z' - \kappa| \sqrt{1 - \frac{2\sqrt{2}}{3} \cos \theta_\vartheta} < \sqrt{3} |\tau z' - \kappa|$ , where the inequality holds since we can either choose  $\vartheta = 1 + i$  or  $-1 - i$  such that  $0 < \theta_\vartheta \leq 90^\circ$ . Furthermore, we have  $|\psi z' - \phi| < \frac{\sqrt{3}}{3} |\tau z' - \kappa| < |\tau z' - \kappa|$ . Therefore, we can prove that  $(\kappa, \tau)$  and  $(\gamma, \delta)$  are non-adjacent for  $|\tilde{\Xi}| = 3$  under *Choice 3*.

## REFERENCES

- [1] S. Zhang, S. C. Liew, and P. P. Lam, "Hot topic: physical-layer network coding," in *Proc. ACM Mobicom*, Sep. 2006.
- [2] S. C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: tutorial, survey, and beyond," *Phys. Commun.*, vol. 6, pp. 4–42, Mar. 2013.
- [3] P. Popovski and H. Yomo, "The anti-packets can increase the achievable throughput of a wireless multi-hop network," in *Proc. IEEE ICC*, Jun. 2006.
- [4] S. Zhang and S. C. Liew, "Channel coding and decoding in a relay system operated with physical-layer network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 788–796, Jun. 2009.
- [5] T. Yang, I. Land, T. Huang, J. Yuan, and Z. Chen, "Distance spectrum and performance of channel-coded physical-layer network coding for binary-input Gaussian two-way relay channels," *IEEE Trans. Commun.*, vol. 60, no. 6, pp. 1499–1510, Jun. 2012.
- [6] H. Yang, Y. Choi, and J. Chun, "Modified high-order PAMs for binary coded physical-layer network coding," *IEEE Commun. Lett.*, vol. 14, no. 8, pp. 689–691, Jan. 2010.
- [7] R. Chang, S. -J. Lin, and W. -H. Chung, "Symbol and bit mapping optimization for physical-layer network coding with pulse amplitude modulation," *IEEE Trans. Wireless Commun.*, vol. 12, no. 8, Aug. 2013.
- [8] L. Yang, T. Yang, J. Yuan, and J. An, "Achieving the near-capacity of two-way relay channels with modulation-coded physical-layer network coding," *IEEE Trans. Wireless Commun.*, vol. 14, no. 9, pp. 5225–5239, Sep. 2015.
- [9] T. Yang and I. Collings, "Asymptotically optimal error-rate performance of linear physical-layer network coding in Rayleigh fading two-way relay channels," *IEEE Commun. Lett.*, vol. 16, no. 7, pp. 758–760, July 2010.
- [10] T. Yang and I. Collings, "On the optimal design and performance of linear physical-layer network coding for fading two-way relay channels," *IEEE Trans. Wireless Commun.*, vol. 13, no. 7, pp. 956–967, Feb. 2014.
- [11] L. Shi, S. C. Liew, and L. Lu, "On the subtleties of  $q$ -PAM linear physical-layer network coding," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2520–2544, May 2016.
- [12] T. K.-Akino, P. Popovski, and V. Tarokh, "Optimized constellations for two-way wireless relaying with physical network coding," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 5, pp. 773–787, June 2009.
- [13] V. Muralidharan, V. Nambodiri, and B. Rajan, "Wireless network-coded bidirectional relaying using Latin squares for  $M$ -PSK modulation," *IEEE Trans. Inf. Theory*, vol. 59, no. 10, pp. 6683–6711, Oct. 2013.
- [14] U. Erez and R. Zamir, "Achieving  $\frac{1}{2} \log(1 + \text{snr})$  on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, 2004.
- [15] B. Nazer and M. Gastpar, "Compute-and-forward: harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6485, Oct. 2011.
- [16] B. Hern and K. R. Narayanan, "Multilevel coding schemes for compute-and-forward with flexible decoding," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7613–7631, Jul. 2013.
- [17] C. Feng, D. Silva, and F. R. Kschischang, "An algebraic approach to physical-layer network coding," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7576–7596, Nov. 2013.
- [18] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proc. IEEE*, vol. 99, no. 3, pp. 438–460, Mar. 2011.
- [19] W. Nam, S. Y. Chung, and Y. Lee, "Capacity of the Gaussian two-way relay channel to within 1/2 bit," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5488–5495, Nov. 2010.
- [20] J. B. Fraleigh, *A First Course in Abstract Algebra*, Reading, MA: Addison-Wesley, 1982.
- [21] K. Conrad, *The Gaussian Integers*, [Online]. Available: <http://www.math.uconn.edu/kconrad/blurbs/ugradnumthy/Zinotes.pdf>.
- [22] *Bézout's Identity*, [Online]. Available: [http://en.wikipedia.org/wiki/B%C3%A9zout's\\_identity](http://en.wikipedia.org/wiki/B%C3%A9zout's_identity).
- [23] J. W. S. Cassels, W. Ledermann, and K. Mahler, "Farey section in  $k(i)$  and  $k(\rho)$ ," *Philos. Trans. Royal Soc. London Ser. A*, pp. 585–628, Aug. 1951.
- [24] J. W. S. Cassels, *An introduction to the Geometry of Numbers*, Berlin, Germany: Springer, 1997.
- [25] A. Okabe, B. Boots, K. Sugihara, and S. N. Chiu, *Spatial tessellations: concepts and applications of Voronoi diagrams*, New York: Wiley, 1992.
- [26] P. F. Ash and E. D. Bolker, "Generalized Dirichlet Tessellations," *Geometriae Dedicata*, vol. 20, no. 2, pp. 209–243, 1986.
- [27] F. Aurenhammer, "Voronoi diagrams - A survey of a fundamental geometric data structure," *ACM Computing Surveys*, vol. 23, no. 3, pp. 345–405, Sep. 1991.
- [28] Quadratic reciprocity, [Online]. Available: [https://en.wikipedia.org/wiki/Quadratic\\_reciprocity](https://en.wikipedia.org/wiki/Quadratic_reciprocity)
- [29] S. Boyd and L. Vandenberghe, *Convex optimization*, Cambridge University Press, 2004.